VBrick
EtherneTV Portal Server

ETV v4.2 Portal Server
Admin Guide

December 14, 2007
4410-0118-0007

Copyright

© 2007 VBrick Systems, Inc. All rights reserved.
12 Beaumont Road
Wallingford, Connecticut 06492, USA
www.VBrick.com

This publication contains confidential, proprietary, and trade secret information. No part of this document may be copied, photocopied, reproduced, translated, or reduced to any machine-readable or electronic format without prior written permission from VBrick. Information in this document is subject to change without notice and VBrick Systems assumes no responsibility or liability for any errors or inaccuracies. VBrick, VBrick Systems, the VBrick logo, StreamPlayer, and StreamPlayer Plus are trademarks or registered trademarks in the United States and other countries. Windows Media is a trademarked name of Microsoft Corporation in the United States and other countries. All other products or services mentioned in this document are identified by the trademarks, service marks, or product names as designated by the companies who market those products. Inquiries should be made directly to those companies. This document may also have links to third-party web pages that are beyond the control of VBrick. The presence of such links does not imply that VBrick endorses or recommends the content of any third-party web pages. VBrick acknowledges the use of third-party open source software and licenses in some VBrick products. This freely available source code is posted at http://www.vbrick.com/opensource.

About VBrick Systems

Founded in 1997, VBrick Systems, an ISO 9001 certified vendor, is a privately held company that has enjoyed rapid growth by helping our customers successfully introduce mission critical video applications across their enterprise networks. Since our founding, VBrick has been setting the standard for quality, performance and innovation in the delivery of live and stored video over IP networks—LANs, WANs and the Internet. With thousands of video appliances installed world-wide, VBrick is the recognized leader in reliable, high-performance, easy-to-use networked video solutions.

VBrick is an active participant in the development of industry standards and continues to play an influential role in the Internet Streaming Media Alliance (ISMA), the MPEG Industry Forum, and Internet2. In 1998 VBrick invented and shipped the world's first MPEG Video Network Appliance designed to provide affordable DVD-quality video across the network. Since then, VBrick's video solutions have grown to include Video on Demand, Management, Security and Access Control, Scheduling, and Rich Media Integration. VBrick solutions are successfully supporting a broad variety of applications including distance learning and training, conferencing and remote office communications, security, process monitoring, traffic monitoring, business and news feeds to the desktop, webcasting, corporate communications, collaboration, command and control, and telemedicine. VBrick serves customers in education, government, healthcare, and financial services markets among others.

Contents

Portal Server v4.2 Admin Guide

Organization ix
Getting Help x
Font Conventions x
Related Documents xi
Printer-Friendly xi

1. Introduction

Portal Server Overview 1
- Server Requirements 2
- Desktop Requirements 2
- Copyright Protection 3
- MySQL 4

Portal Server Features 4
- End User Features 4
- Administrative Features 5

Portal Server Components 6
- VBrick Encoders/Decoders 6
- ETV Video-on-Demand Servers 6
- ETV Set Top Box 8
- ETV Network Video Recorder 8
- VB-PC Remote Controller 9
- Amino Set Top Box 9
- WM IP Receiver 10

Portal Server Installation 10
- Download Components 10
- Port Requirements 12
- Portal Server License Files 14

Admin Console Login 15
- Admin Console Options 16
- Internet Explorer 7.0 Configuration 18

2. Global Settings

Global Assignments 19
Custom Fields 25
Stream Restrictions 26
Servers 27
- Using Secure FTP 27
- Add/Modify VOD/FTP Servers 28
- Add/Modify Video On Demand Content Folders 34

VBricks 36
- Advanced Settings 38

Control Devices 38
Adding Control Devices 39
Adding User-Defined VBIRs 41
Connecting Control Devices 42
Configuring Control Devices 43
Control Device VBIRs 43
Set Top Boxes 44
Recorders 46
Synchronizing the Portal Server and the NVR 47
Script Devices 48
Scripts 49
Creating a Script 50
Finding VBrick Parameters and Values 52
URLs 52
Add/Modify a URL for a Live Video Stream 52
Add VOD Content 54
Add Non-VOD Content 55
Emergency Broadcast 55
Program Names 59
Manage Playlists 60
Access Logging 61
Extended Logging Properties 62
Viewing the Access Logs 62

3. Server Administration

Channels 65
Channel Guide 65
Stations 66
Custom Programs 71
Modify VOD Content 73
Diagnostics 75
Status 75
Expired Content Log 76
Access Control 76
Using LDAP Servers 77
Using Single Sign-On 79
Using LDAP Servers with SSL 81
Live Presentations 83
Users 84
User Groups 84
Resource Groups 84
Help 84
Logout 85

4. Users and User Groups

Overview 87

Definitions 87
Configuring Users and User Groups 89
1. Setup and Configure ETV Components 89
2. Choose an Authentication Method 89
3. Create User Groups on the Portal Server 90
4. Create Resource Groups on the Portal Server 91
5. Create Users on the ETV Portal Server 91
6. Assign Resources to Users or User Groups 91
Configuring Users 91
Add/Modify User Information 93
Add/Modify User's Group Assignments 94
Add/Modify User's Resource Group Assignments 94
Add/Modify Live Channel Privileges 94
Allow Access to Specific FTP Servers 95
Allow Access to Specific Recorder Servers 95
Allow Access to Specific VOD Servers 95
Allow Access to Specific VOD Content 95
Allow Viewing by Content Type 95
Allow Content Publishing 96
Allow Content Recording 96
Default Content Recording 96
Allow VBrick Access 96
STB Access 96
Schedule Privileges 97
Emergency Broadcast Privileges 97
Copyright Restrictions & Expiration Privileges 97
Configuring User Groups 97
Add/Modify Group Information 98
Add/Modify Group's User Assignments 98
Add/Modify Group's Resource Assignments 98
Resource Groups 99
Add/Modify Resource Group Information 99
Add/Modify User's Resource Assignments 100
Add/Modify Group's Resource Assignments 100
STB Authentication 100
Authentication by PIN 100
Authentication by Host Name or IP Address 101

5. Configuring for SSL

Overview 103
1. Generate a Certificate Request 103
2. Submit a Certificate Request 104
3. Install the Certificate 104
4. Configure ETV Resources for SSL 105

6. Network Video Recording

NVR Overview 107
NVR Hardware 108
NVR Performance Considerations 109
NVR Types 109
Standard NVR 109
Standalone NVR 109
NVR Installation 110
Synchronizing the Portal Server and the NVR 110
NVR Configuration 110
Configuring a Standard NVR 110
Configuring a Standalone NVR 111
Using an NVR 111

7. VBPresenter

Overview 113
Working with Presentations 114
Configuring MCS for VBPresenter 114
Configuring an FTP User 114
Configuring a Presentation User 114
Configuring for Live Presentations 115
Configuring for Stored Presentations 117

8. Auto Content Ingestion

AutoIngest Content 119
AutoIngest Content via XML 121
AutoIngestXML Modes 122
Using the XML Template 122
Removing MPEG-4 Closed Captions 124

9. Database Backup

Introduction 125
Database Backup 125
Database Restore 126

10. Amino Set Top Box

Overview 127
Connecting the Amino 127
Configuring the Amino 128
Changing the IP Address 129
Configuring a Direct Connection 129
Configuring the Remote Control for a TV 130
Configuring the Amino for a Widescreen 130
Setting the TV Display Format 130

11. ACNS Configuration

Overview 133
ACNS Configuration 133
VOD-W Server Configuration 133
Portal Server Configuration 134
ACNS Server Configuration 135
Verify Installation. 135

12. Rebranding the User Interface

Customizing the Portal Server 137
Changing the Title and Header Image 137
Rebranding the Portal Server 138
Portal Server 138
Rebranding Other ETV Components 142
VBrick Set Top Box 142
Amino Set Top Box 142
VBrick IP Receiver 142

13. NXG-to-VOD-W Content Migration

Creating an Asset List 143
Sample Asset List 144
Using the Migration Tool. 144
Increasing the Ingestion Rate 145
Running the Migration Tool 145
Recovering from Migration Errors 147
Verifying the Migration 147

Index

Portal Server v4.2 Admin Guide

This *Portal Server Admin Guide* is written for anyone who will be using or evaluating the VBrick EtherneTV Portal Server. This includes system administrators, software developers, network technicians, and others. The ETV Portal Server is a web-based portal for accessing and managing video assets including both live or stored audio and video files. The ETV Portal Server is a key component in VBrick's EtherneTV Media Distribution System. The ETV Portal Server provides a simple, intuitive interface that auto-discovers available media assets in your network. Key components in VBrick's EtherneTV solution include:

- **EtherneTV-VOD Video-on-Demand Server** – Provides all standard Video-on-Demand (VOD) features including support for MPEG-1, MPEG-2, MPEG-4, and Windows Media for maximum flexibility.
- **EtherneTV Digital IP Receivers** – Leading edge digital set top boxes that provide a low-cost standalone decoder for DVD-quality MPEG-1, MPEG-2, MPEG-4, and Windows Media video assets.
- **VBrick Hardware Encoders/Decoders** – Rugged, reliable video appliances that can reside anywhere on your network to provide either distributed or high-density centralized encoding/decoding of MPEG-1, MPEG-2, MPEG-4, and WM (Windows Media) video.

Note The Amino STB is a compact set top box that plays MPEG-2 streams only. It is fully integrated with the Portal Server and provides access to *most* Portal Server viewer functionality. *It does not, however, support* Access Logging, Scheduling, Device Control, Emergency Broadcast, or Copyright Restrictions.

Organization

Introduction	provides an overview of the application including server and desktop requirements and an overview of features and functionality.
Global Settings	explains high-level configuration settings and parameters that apply to the entire system.
Server Administration	provides detailed explanations of all ETV Portal Server global settings and configuration options, as well as diagnostics and status windows.
Users and User Groups	explains how to configure the system for access control. It explains how to create users and groups with specific permissions and access to resources.
Configuring for SSL	explains how to securely configure the system using the Secure Sockets Layer.
Network Video Recording	explains how to configure and use an NVR to offload recording tasks from the Portal Server to a separate "recorder server" machine.

VBPresenter	explains how to configure and launch rich media presentation from the Portal Server including those created with VBPresenter.
Auto Content Ingestion	explains auto content ingestion. This is the process whereby video content is automatically populated on the portal server.
Database Backup	explains how to backup the MySQL database when you transfer or remove VOD servers. Note that procedure backs up the database—not video content.
Amino Set Top Box	explains how to connect and use the Amino set top box to view MPEG-1 and MPEG-2 streams.
ACNS Configuration	explains how to configure the Portal Server and Cisco's Application and Content Networking System (ACNS) to work together.
Rebranding the User Interface	explains how to modify the Portal Server "user" interface. You can simply replace images or you can modify the .css stylesheets and thoroughly rebrand the look-and-feel of the application.
NXG-to-VOD-W Content Migration	explains how to migrate MPEG-1 and MPEG-2 video files from a VBrick NXG (Linux) VOD server to a VBrick VOD-W (Windows) VOD server.

Getting Help

If you need help, or more information about any topic, use the online help system. The online help is cross-referenced and searchable and can usually find the information in a few seconds. Use the tree controls in the left pane to open documents and the up and down arrows to page through them. Use the **Search** box to find specific information. Simply enter one or more words in the box and press Enter. The search results will return pages that have all of the words you entered—highlighted in yellow (Internet Explorer only). The **Search** box is not case-sensitive and does not recognize articles (a, an, the), operators (+ and –), or quotation marks. You can narrow the search by *adding* words.

If you can't find the information you need from the online help, or from your certified VBrick reseller, you can contact VBrick Support Services on the web. Support Services can usually answer your technical questions in 24 business hours or less. Also note that our publications team is committed to accurate and reliable documentation and we appreciate your feedback. If you find errors or omissions in any of our documents, please send e-mail to documentation@vbrick.com and let us know. For more information about any VBrick products, all of our product documentation is available on the web. Go to www.vbrick.com/documentation to search or download VBrick product documentation.

Font Conventions

Arial bold is used to describe dialog boxes and menu choices, for example: **Start > All Programs > VBrick**

`Courier fixed-width font is used for code elements (C++, HTML) as well as filenames, directories, etc.`

`Black Courier fixed-width font is used to indicate user input in keyboard commands, scripts, etc.`

Folder names and user examples are displayed in this sans serif font.

Folder names and user input are displayed in this bold sans serif font.

Italics are used to emphasize specific words or phrases.

Related Documents

ETV Portal Server User Guide

ETV IPR Receiver Admin Guide

ETV STB Admin Guide

ETV STB Quick Start Guide

ETV NXG Server Quick Start Guide

ETV VOD W Server Quick Start Guide

ETV VOD WM Server Admin Guide

VBPresenter User Guide

Printer-Friendly

Click on the following link to print a hard copy of the document.

ETV Portal Server User Guide

ETV Portal Server Admin Guide

ETV Portal Server Release Notes

▼ To save or print a PDF document:

1. Click once to open the PDF document in Acrobat Reader.
2. To save or print a PDF document, right-click and select **Save Target As** or **Print Target**.

Chapter 1F

Introduction

Topics in this chapter

Portal Server Overview 1
Portal Server Features 4
Portal Server Components 6
Portal Server Installation 10
Admin Console Login 15

Portal Server Overview

VBrick's EtherneTV Media Distribution System consists of a group of products that includes the EtherneTV Portal (ETV Portal Server), EtherneTV Encoders, the EtherneTV-VOD Video-on-Demand Server, EtherneTV Set-Top Boxes and StreamPlayer software. This integrated system delivers both live and on-demand audio and video over an IP-based infrastructure. The ETV Portal Server functions as a video portal, permitting end users to view live and on-demand MPEG-1, MPEG-2, MPEG-4 and WM (Windows Media) streams on a Window PC, a Macintosh, a Linux PC (or a set top box). The ETV Portal Server comes as software-only solution that can be installed on a Windows Server or as a pre-configured hardware/software combination.

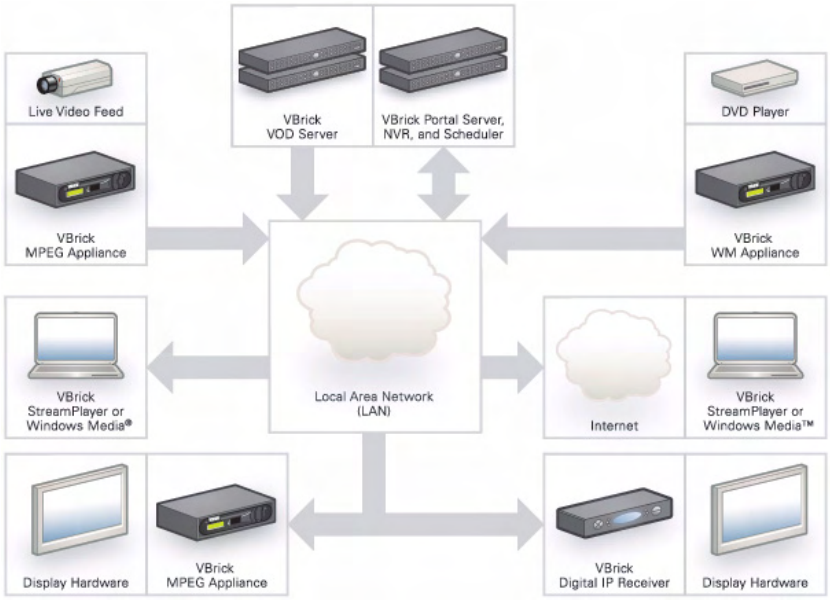


Figure 1. EtherneTV Media Control Server Suite

The VBrick EtherneTV (ETV) Portal Server is a web-based portal for accessing Live and On-Demand audio and video files. A key component of VBrick's EtherneTV Media Distribution System, the ETV Portal Server provides a simple interface to easily locate

available media assets on your network. Upon accessing the main portal page, users can navigate or search for specific videos, select the video, and immediately begin viewing DVD quality video. For on-demand videos, users can **Fast Forward/Rewind** and **Seek** to specific points in the video. Standard access control functionality provides restriction of certain content to particular users, user groups, or set top boxes. An optional scheduling module allows users to schedule devices to send video, receive video, record video, or to initiate a two-way conference.

Server Requirements

The *minimum* server requirements include:

- Windows Server 2003 (Web Edition or Standard Edition with Service Pack 2).
- Pentium IV or Xeon Processor 1.26 GHz Minimum (2 GHz or higher recommended).
- RAM 512 MB Minimum (1 GB or more recommended).
- Hard Drive 36 GB Minimum (larger for frequent recording).

Note VBrick has tested the ETV Portal Server on Windows 2000 Web Server and on Windows 2003 Server Web Edition and Standard Edition. Note also that ETV Portal Server also will not operate correctly on a server that is configured as a primary domain controller or with other network-related services and software.

Desktop Requirements

Windows-based PC and Macintosh users access the ETV Portal Server through a web browser. For Windows-based PCs, on the first access to the server, VBrick StreamPlayer software is automatically downloaded to the PC. StreamPlayer software lets end users select a stream and view TV-quality video directly on a PC. Macintosh users view MPEG-4 video through the QuickTime player.

Table 1. Desktop Requirements

PC Type	Requirements
Windows PCs	• Windows 2000, XP (Service Pack 2), or Vista. • 300 MHz Pentium II processor for MPEG-1 streams. • 500 MHz Pentium III processor for MPEG-2 streams. • 500 MHz (minimum), 750 MHz Pentium III processor (recommended) for MPEG-4 streams. • 128 MB RAM. • SVGA video card 640x480, 256 colors, video card acceleration recommended. • Minimum 10 MB hard disk space for installation. • Microsoft Internet Explorer 6.0 or higher. • Microsoft Windows Media Player 9.0 or higher. • Firefox 1.0 or higher. • DirectX Media Version 8.1 and higher.

© 2007 VBrick Systems, Inc.

PC Type	Requirements
Macintosh PCs	• Mac OS X with Safari 1.0 or higher. • Firefox for Macintosh 1.0.4 or higher. • QuickTime Player 6.0 or higher. • Internet Explorer on a Macintosh is not supported.
Linux PCs	• Red Hat Fedora Core 3. • FireFox 1.0. • 512 MB RAM.

Copyright Protection

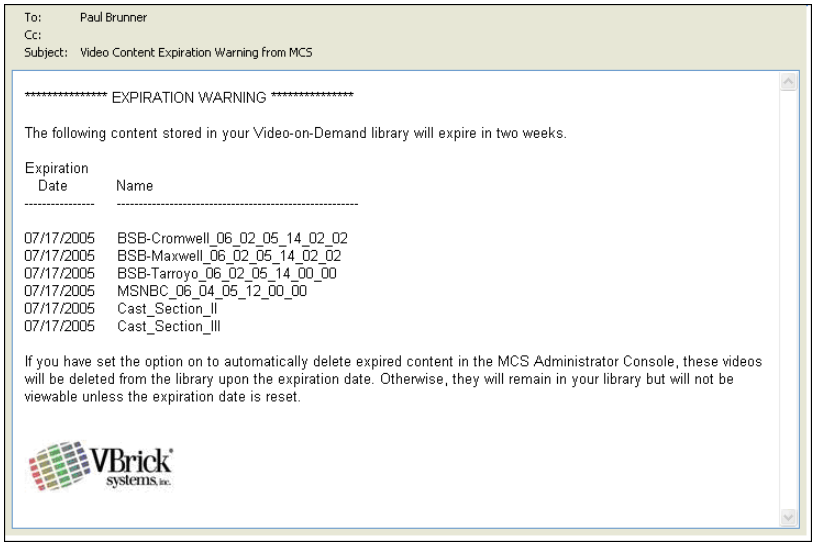
The Portal Server uses copyright restrictions and content expiration to protect the rights of content owners and to enforce rules against unauthorized usage or distribution. Copyright restrictions are specifically used to enforce license requirements. Content is often restricted to a limited number of viewers and you may need a license, for example, to view MPEG-2 content. In the Portal Server, **Max. Concurrent Viewers** is used to enforce copyright restrictions for any live, stored, or recorded video. If the number of concurrent viewers exceeds the configured value, the content will not play. (The **Max. Concurrent Users** restriction does not apply to viewers who tune in to a scheduled broadcast.)

Content expiration controls the length of time that specific content can be viewed. Content expiration is used for time-sensitive, copyrighted, or otherwise protected content that cannot be legally displayed after a specified date or a period of time. Users with appropriate permissions (see Copyright Restrictions & Expiration Privileges on page 97) can assign expiration dates or a viewing period when they use the **Add Video** feature. The viewing period starts at the time the content is added to the server. If desired, administrators can restrict expiration privileges to particular users or groups in which case only those specified users or groups (and administrators) can set content to expire.

Administrators can also assign an **Expiration Date** or **Viewing Period** for any stored video using the Modify VOD Content page. By default, recordings from live streams have no expiration date. However administrators can set default viewing periods for content recorded from specific live streams (see "Viewing Periods" in Stream Restrictions on page 26).

The ETV Portal Server enforces content expiration by preventing the streaming or scheduling of content that is expired or will expire before the scheduled event. Once content has expired, administrators can set a new expiration date or viewing period. By default, expired content will remain in storage indefinitely unless you choose to delete it automatically using the **Set Expired VOD Content Treatment** option in Global Assignments.

The Portal Server writes to a log that tracks content expirations; administrators can view or purge this log as necessary (see Expired Content Log on page 76). In many installation an administrator is assigned to monitor and/or renew content that is about to expire. To facilitate this process, the Portal Server can be configured to automatically generate e-mail that notifies the designated administrator when content is about to expire by using the option in Global Assignments.



To: Paul Brunner
Cc:
Subject: Video Content Expiration Warning from MCS

********** EXPIRATION WARNING **********

The following content stored in your Video-on-Demand library will expire in two weeks.

Expiration Date	Name
07/17/2005	BSB-Cromwell_06_02_05_14_02_02
07/17/2005	BSB-Maxwell_06_02_05_14_02_02
07/17/2005	BSB-Tarroyo_06_02_05_14_00_00
07/17/2005	MSNBC_06_04_05_12_00_00
07/17/2005	Cast_Section_II
07/17/2005	Cast_Section_III

If you have set the option on to automatically delete expired content in the MCS Administrator Console, these videos will be deleted from the library upon the expiration date. Otherwise, they will remain in your library but will not be viewable unless the expiration date is reset.

VBrick systems, inc.

MySQL

EtherneTV Portal Server is shipped with MySQL as the database. The MySQL database is installed as part of the Portal Server installation package. If the hardware/software combination was purchased from VBrick, MySQL will already be installed on your machine; the default user name is `root`. To protect the integrity of the database, you should change the default password (`vbrick_18`) after initial installation and periodically thereafter as explained below. To backup the MySQL database, see Database Backup on page 125.

Note MySQL Query Browser is an Open Source front-end that provides a graphical interface to the MySQL database. MySQL Query Browser is available with the free software/open source GNU General Public License at to http://www.mysql.com.

▼ To change the MySQL password:

1. Open a Command Prompt window.
2. At the C: prompt type **`cd program files\mysql\mysql server 4.1\bin`** and press **Enter**.
3. Type **`mysql -uroot -pvbrick_18`** and press **Enter**.
4. Type **`set password for 'root'@'localhost'=password ('new_password');`** (where **`'new_password'`** in single quotes is the new password) and press **Enter**.
5. Type **`exit`**.

Portal Server Features

End User Features

- Windows-based PCs, Macintoshes, or STBs (connected to televisions or display monitors) can all access the Portal Server.
- Users can view video at **Full Screen** for a television-like user experience.
- Users can view Video-On-Demand assets with full VCR/DVD control, including **Play**, **Pause**, **Stop**, **Fast Forward**, **Rewind**, and **Seek**.
- Video can be viewed in a preview window or launched in multiple external, re-sizeable player windows (PC and Macintosh).

© 2007 VBrick Systems, Inc.

- Set Top Box users can use familiar **Channel Up/Down** keys and other hot keys on the IR remote control to navigate through video listings.
- Users can search through the list of Live or On-Demand videos by **Title**, **Keyword**, **Description**, or other custom fields defined by an ETV Portal Server administrator.
- Users can record and store videos on the EtherneTV-VOD Video-on-Demand server via ETV Portal Server.
- Users can publish pre-recorded content and thumbnails directly to the VOD server.
- Users can view closed caption text (Windows-based PCs and set-top boxes only).
- Users can launch pre-configured emergency broadcasts. (Optional. Requires Scheduling module.)
- Users can schedule recordings or broadcasts. (Optional. Requires Scheduling module.)

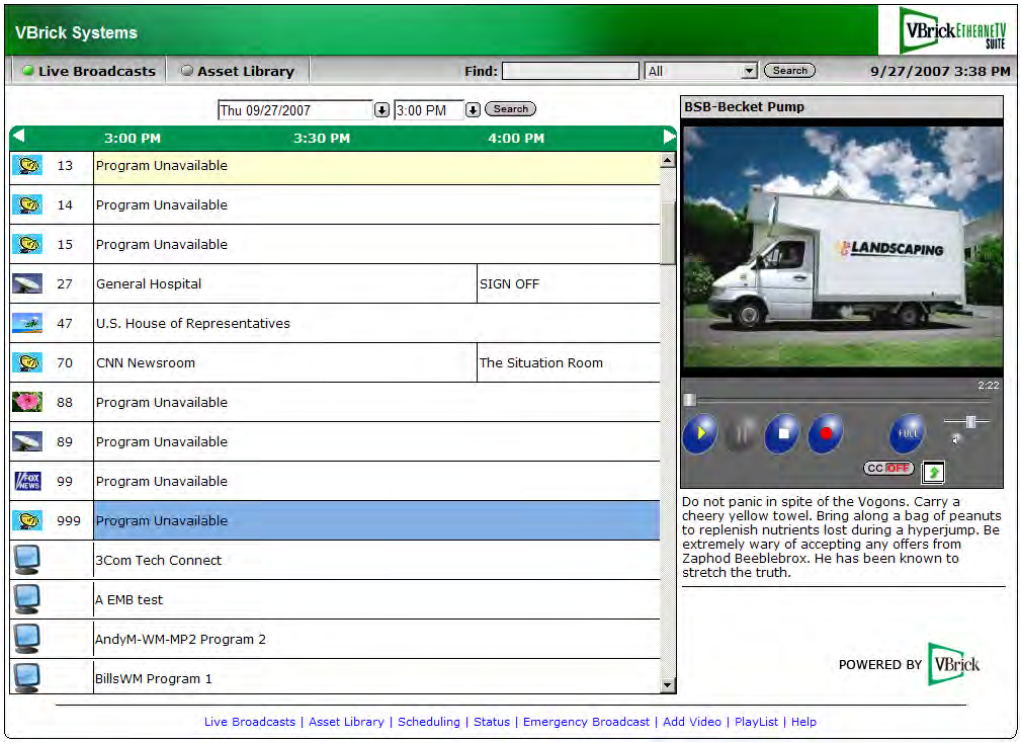

VBrick Systems
Live Broadcasts
Asset Library
Find:
All
Search
9/27/2007 3:38 PM
Thu 09/27/2007
3:00 PM
Search
3:00 PM
3:30 PM
4:00 PM
13 Program Unavailable
14 Program Unavailable
15 Program Unavailable
27 General Hospital
SIGN OFF
47 U.S. House of Representatives
70 CNN Newsroom
The Situation Room
88 Program Unavailable
89 Program Unavailable
99 Program Unavailable
999 Program Unavailable
3Com Tech Connect
A EMB test
AndyM-WM-MP2 Program 2
BillsWM Program 1
BSB-Becket Pump
LANDSCAPING
2:22
Do not panic in spite of the Vogons. Carry a cheery yellow towel. Bring along a bag of peanuts to replenish nutrients lost during a hyperjump. Be extremely wary of accepting any offers from Zaphod Beeblebrox. He has been known to stretch the truth.
POWERED BY VBrick
Live Broadcasts | Asset Library | Scheduling | Status | Emergency Broadcast | Add Video | PlayList | Help

Figure 2. ETV Portal Server Live Broadcasts

Administrative Features

- Access Control - allows administrators to allow/deny access to specific functions of the ETV Portal Server server. Access control functionality can use the local ETV Portal Server database or authenticate to an LDAP directory server.
- Clustering support – multiple EtherneTV-VOD Video-on-Demand servers can be clustered to increase total throughput. The ETV Portal Server will automatically load balance all servers defined in ETV Portal Server; no additional configuration is necessary. See Servers on page 27 for more.
- SSL/TLS security – the ETV Portal Server can be set up to provide encrypted access to the Login pages and/or the Admin pages. See Configuring for SSL on page 103.
- Customer defined URLs – can be entered into the system and displayed in the ETV Portal Server interface. The URLs can point to video assets or other assets such as PDFs or PowerPoint documents.

- Autoingestion to the EtherneTV-VOD server – content placed in autoingestion folders on the ETV Portal Server will be automatically transferred and ingested into the EtherneTV-VOD server.
- Customized global messages can display on the ETV Portal Server interface.
- Channel numbers can be assigned to live streams.
- Define a startup channel for STBs – the STB will automatically tune into this channel when users select the **Live TV** option.
- Emergency broadcasts – can define pre-configured emergency broadcast templates that can be launched instantaneously. See Emergency Broadcast on page 55 for more.
- Status window – shows the status of videos being added, recorded, or ingested.
- Diagnostics window – displays a complete log of system events by source, time, and IP address.
- Custom fields and streams – the ability to add customized information and search parameters to live and stored streams.
- A Channel Guide Server can be configured to automatically provide third-party programming data for configured TV Stations.

Portal Server Components

VBrick Encoders/Decoders

VBrick's VB4000-5000-6000 Series MPEG-2 network video appliances provide DVD quality video and CD quality audio at 1–15 Mbps of bandwidth. MPEG-2 is the world's most popular digital compression technology and is used to encode DVDs as well as Digital Cable and Digital Satellite broadcasts. VBrick's VB4000-5000-6000 Series MPEG-4 encoders and decoders are versatile and reliable video appliances for one or two-way interactive communications over low or medium bandwidth IP networks. The VBrick MPEG-4 encoder/decoder can be used for webcasting, multicasting, transcoding, and two-way interactive video. Designed for streaming over the Internet at lower bit rates (56K, 128K, 384K) and over a LAN at higher rates (1Mbps and above). VBrick's WM (Windows Media) video appliances provide scalable quality at webcasting rates up to 2 Mbps. It features built-in live streaming server, automatic multicasting, and state-of-the-art reliability. A key benefit of the WM appliance is its compatibility with the Windows Media Player, thus eliminating the need for desktop player installation.

ETV Video-on-Demand Servers

EtherneTV Video on Demand (VOD) servers provide the ETV Portal Server with a source of available video content organized in folders. The VOD content is displayed by name in the ETV Portal Server user interface, along with the duration of the video, and associated descriptions, key words, and other custom information entered by an administrator. You play content from the VOD server by selecting the program name from the application interface (see the *Portal Server User Guide* for details). The ETV Portal Server currently supports all of the VOD servers shown in Table 2. The configuration for each server is essentially the same (see Servers on page 27 for details) and there is little difference in functionality for end users.

ETV servers can be LAN-based or Internet-based depending on how the range of Internet addresses is defined (see "Assign LAN/Internet Address Range" in Global Assignments on page 19). VOD servers accessible to Internet users are called Internet-zone servers; VOD

© 2007 VBrick Systems, Inc.

servers assessable to LAN users only (within a secured corporate network and behind a firewall) are called LAN-zone servers.

Content added by users in the LAN zone will be ingested to all VOD servers for which they have permissions using the **Add Video** page. Users in the Internet zone have the **Add Video** page available only if they have permissions for at least one VOD server that is also in the Internet zone. Content added by LAN users is added to all configured servers that can handle the content (for example you cannot add MPEG content to a Windows Media server) and for which you have permission. The content available for viewing may also be limited by the server type. For example, Internet users will see only MPEG-4 and Windows Media content on VOD-D and VOD-WM servers respectively. LAN users however will see all content on all servers.

Table 2. Supported EtherneTV VOD Servers

Server Type	Description	Zone
NXG	Linux-based NXG1/2 VOD server.	LAN only
VOD-W	Windows-based VOD-W VOD server.	LAN only
VOD-D	Darwin Open Source server for Linux, Windows, Mac, etc. Ingests and plays MPEG-4 content only. Requires an FTP server.	LAN or Internet
VOD-WM-Standard	Microsoft Windows Media Server (unicast only). Requires an FTP server.	LAN or Internet
VOD-WM-Enterprise	Microsoft Windows Media Server (unicast or multicast). Requires an FTP server.	LAN or Internet

ETV Internet-Based Servers

ETV Portal Server supports the installation of LAN-based servers and Internet-based servers. As part of an ETV Server installation, you can configure a VOD-D or VOD-WM server (see Table 2) to run on your LAN or on the public Internet. Before server configuration, you assign a range of IP addresses that define the LAN domain, or vice versa, that define the Internet domain. Any IP address outside that range will assumed to be from an Internet source, or vice versa, from a LAN source. (See "Assign LAN/Internet Address Range" in Global Assignments on page 19.)

You can purchase an Internet-based Windows Media server from VBrick (in which case it is configured by VBrick) or you can purchase and configure it yourself using the Microsoft documentation (not recommended). You can also install a Darwin Open Source server which is fully-compatible with ETV Portal Server but is not sold or supported by VBrick. (For more about downloading, installing, and configuring a Darwin server, go to: http://developer.apple.com/opensource/server/streaming/index.html) As noted, ETV users can be on the Internet or on a LAN; Internet users can only access MPEG-4 and Windows Media content stored on Internet-based servers. LAN users can access all content on all servers both inside and outside the firewall. To summarize, *Internet-based* servers and users are subject to the following limitations:

- Internet servers support MPEG-4 and Windows Media content only.
- Internet servers support unicast only (they do not support multicast).
- Internet ETV users can add video only to VOD servers in the Internet zone.

- Internet users can only see MPEG-4 and Windows Media content stored on Internet-based servers.
- Internet servers do not support ETV scheduling features.

ETV Set Top Box

EtherneTV-STBs access the ETV Portal Server through a web browser within the Set Top Box. Using the Set-Top Box remote control, users can navigate and search for specific on-demand content or live video streams, select a stream, and begin viewing television-quality video. Set-Top Box users can also record video directly on the ETV Portal Server using the remote control or the wireless keyboard. See the Set Top Box documentation for more about how to configure and use an ETV Set Top Box.

ETV Network Video Recorder

The ETV Network Video Recorder and the ETV Live Portal Server are optional components that are purchased and installed separately. They have different license files that must be installed separately. See Portal Server License Files on page 14. The ETV Network Video Recorder lets you off-load all recording tasks from the ETV Portal Server machine to one or more separate "recorder server" machines. This optimizes recording performance and improves ETV Portal Server performance as well. The Network Video Recorder uses ETV Portal Server components and typically requires two machines: the ETV Portal Server is installed on one machine; the Network Video Recorder software is installed on a different machine. Once installed, the NVR machine is used for all ETV Portal Server recording tasks. See Network Video Recording on page 107 for more information.

Note A standard ETV Portal Server permits two concurrent recording operations. If you purchase a Network Video Recorder, the number of concurrent recording operations (10 or 40) is fixed by the terms of your licensing agreement with VBrick.

© 2007 VBrick Systems, Inc.

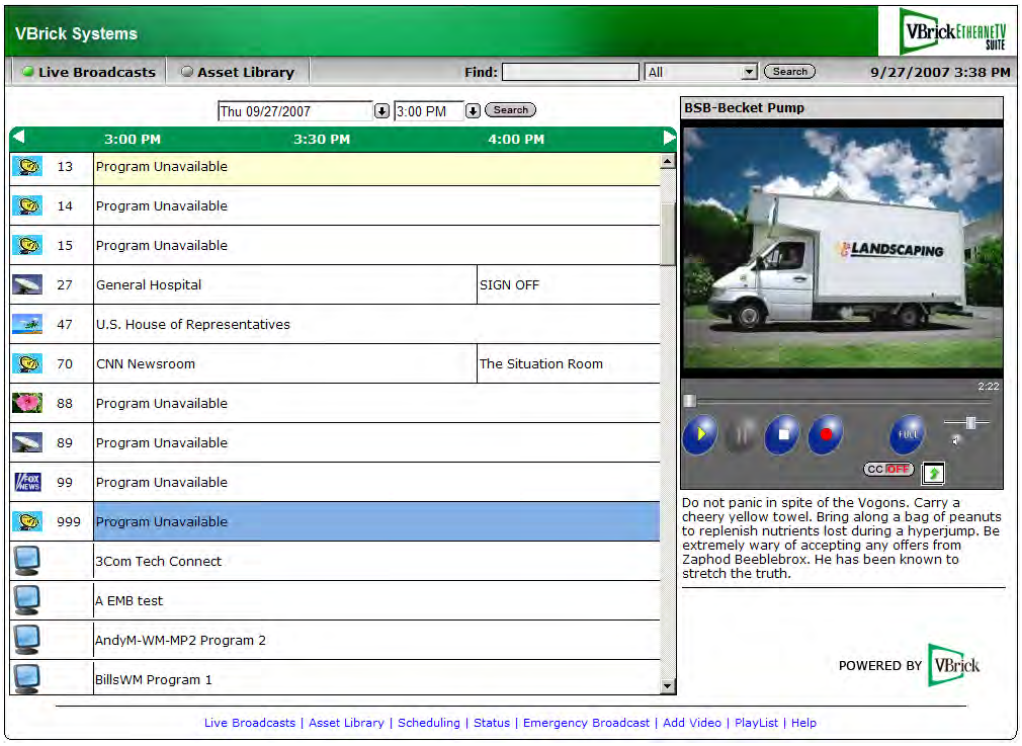

VBrick Systems
Live Broadcasts
Asset Library
Find:
All
Search
9/27/2007 3:38 PM
Thu 09/27/2007
3:00 PM
Search
3:00 PM
3:30 PM
4:00 PM
13 Program Unavailable
14 Program Unavailable
15 Program Unavailable
27 General Hospital
SIGN OFF
47 U.S. House of Representatives
70 CNN Newsroom
The Situation Room
88 Program Unavailable
89 Program Unavailable
99 Program Unavailable
999 Program Unavailable
3Com Tech Connect
A EMB test
AndyM-WM-MP2 Program 2
BillsWM Program 1
BSB-Becket Pump
LANDSCAPING
2:22
Do not panic in spite of the Vogons. Carry a cheery yellow towel. Bring along a bag of peanuts to replenish nutrients lost during a hyperjump. Be extremely wary of accepting any offers from Zaphod Beeblebrox. He has been known to stretch the truth.
POWERED BY VBrick
Live Broadcasts | Asset Library | Scheduling | Status | Emergency Broadcast | Add Video | PlayList | Help

Figure 3. Live Portal Server User Interface

VB-PC Remote Controller

The VB-PC Remote is a handheld infrared device you can use to control (stop/start/pause, etc.) any stream running on the Portal Server. The VB-PC Remote is compatible with Internet Explorer 6.0 or higher; it is not compatible with Firefox. The VB-PC Remote can be used for all Portal Server streams (MPEG-1, MPEG-2, MPEG-4, and WM) and has a line-of-sight range of approximately 40 feet.

After you *manually* start a stream using the Portal Server interface, you can use the VB-PC Remote to control it. When using the remote controller, the computer running the Portal Server basically acts like a set top box that you can control with the remote control. The VB-PC Remote includes an IR Remote Control and an IR Remote Receiver. The computer to which it's attached must have an available (1.1 or 2.0) USB port. Note that the VB-PC Remote is installed on client machines connected to the Portal Server. *It is not part of the Portal Server installation and must be installed separately on each client machine*. See the *VB-PC Remote Product CD* for details and installation instructions.

Amino Set Top Box

The AmiNet110 is a compact set top box for the Portal Server manufactured by Amino Systems. It connects to a standard TV and only plays MPEG-1 and MPEG-2 streams; no other streams are selectable for viewing on the Portal Server interface. There is no software installation required. Simply connect and configure the device as explained in Amino Set Top Box on page 127. The *Portal Server User Guide* explains how to use the Amino infrared remote control unit that comes with the device.

WM IP Receiver

VBrick's WM IP Receiver is similar to a conventional set top box but is significantly more stable, rugged, and reliable. It is designed for 24x7 operation, and built for enterprise networks that require a high degree of stability, security, and scalability. The WM IP Receiver is a robust, state-of-art device that meets the demanding requirements of VBrick's EtherneTV Media Distribution System. The WM IPR plays Windows Media streams from VBrick WM appliances and Windows Media servers. The WM IPR is also a fully-featured VBrick EtherneTV client. This means that in addition to the ability to deliver video, subsequent WM IPR releases will provide scheduling, access logging, and device control from the Portal Server. For more information about the WM IPR, see the *IPR Admin Guide* in the Portal Server online help.

Portal Server Installation

Complete installation instructions for the Portal Server are provided in the *ETV Portal Server Release Notes*. Once the Portal Server is installed, end users on Windows, Macintosh, and Linux machines may be prompted for additional download components as explained below. This only happens the first time they access the Portal Server. The Portal Server supports a wide variety of clients and video formats. See Supported VBrick Clients and Video Formats for a complete list.

Download Components

Windows PCs

If configured with the appropriate components, Windows PCs (with Internet Explorer or Firefox) can play all stream types including MPEG-1, MPEG-2, MPEG-4, and Windows Media. For Windows-based PC users, the Portal Server uses VBrick StreamPlayer software-based components to decode video streams on user desktops. The Portal Server downloads these components to each client machine the first time you access the Portal Server (depending on the **Specify Components to Download to Clients** setting in Global Assignments). No download is necessary for subsequent access. If this is a new installation, end users must answer Yes to security requests to download these components. After a download, you don't have to restart your computer but must you must close the browser. These components are downloaded using .cab files.

In certain circumstances however, the use of .cabs is either not allowed or not feasible. In these cases, VBrick provides an `.msi` installer called `VBrickComponents.msi`. This installer installs the same components and allows end-users who cannot download .cabs to have full Portal Server functionality. This installer is located in the `Program Files\VBrick\MCS\utils` folder.

Note The component download setting will not affect previously-installed components. For example if you have StreamPlayer installed, you will be able to play MPEG-2 streams regardless of what components you specify for download.

With Firefox, users will also be prompted to install additional components the first time they launch a stream—if they are configured to receive these download components. Links for the appropriate stream types (MPEG-1/2/4 and/or WM) will be displayed in the area where the embedded player is normally displayed. These additional plugins *must* be installed. Firefox

© 2007 VBrick Systems, Inc.

users will also be required to install an additional plugin when they use **Add Video** for the first time (again, if they are configured with this privilege).

Table 3. Supported Operating Systems and Browsers – Windows

Operating System	Browser
Windows 2000	Internet Explorer 6.0†, Firefox 1.0†
Windows XP	Internet Explorer 6.0†, Firefox 1.0†
Windows Vista	Internet Explorer 6.0†, Firefox 1.0†

† or higher

Locked-Down Windows PCs

As described above, the Portal Server automatically downloads components to client PCs depending on the Global Assignment setting. This download can be an issue in environments that have restrictions on client software installation. For playback of WM files, Portal Server uses the existing Windows Media Player components on the client PC and there is no need for the extra components to be downloaded. This means that Portal Server and WM can be used in some but not all restrictive or "locked-down" environments.

Even if downloads are configured, a client PC will still refuse to accept the component download if the Internet Explorer security feature **Download signed ActiveX controls** is disabled. When using Portal Server 4.0 exclusively with WM streams and a WM VOD, the client PC can refuse to accept the downloaded components and all Portal Server features except **Add Video** will work. In this case you should uncheck the **Add Video Utility** in Global Assignments.

Some sites also require that their PCs be configured with certain Internet Explorer security settings. The Portal Server will not work on clients with Internet Explorer security set to **High**. The Portal Server *will* work at any level at or below **Medium**. If you start at **High**, the client will still work with Portal Server if you enable **Run ActiveX controls and plug-ins**, **Script ActiveX controls marked safe for scripting**, and **Active scripting**.

Since firewalls on LAN client PCs can also cause problems with Portal Server, it is recommended that firewalls be disabled on LAN clients. (In Windows XP with Service Pack 2, the firewall is enabled by default.) Portal Server's support for Internet clients is designed to work through firewalls. If you have Internet clients with firewalls see the description of LAN/Internet address ranges in Global Assignments on page 19.

Macintosh PCs

If configured with the appropriate components, Macintosh PCs (with Safari or Firefox) can play all stream types including MPEG-1, MPEG-2, MPEG-4, and Windows Media. In a Macintosh environment, if downloads are configured in Global Assignments, when you launch the ETV Portal Server for the first time, the Home page (see Figure 2) displays a link prompting you to download components that are appropriate for your computer. If you agree, these components are automatically installed and no additional download is necessary for subsequent access. On Macintosh PCs, Portal Server functionality is the same as in Windows except that the **Add Video** feature is not available. Table 4 shows the stream types supported for each environment; Table 5 shows the operating systems that are tested and supported. Note that there are certain performance limitations in Macintosh environments; see the *ETV Portal Server Release Notes* for information and recommendations.

Linux PCs

If configured with the appropriate components, Linux PCs running Fedora or Red Hat (on Firefox) can play MPEG-1, MPEG-2, MPEG-4, and WM streams. However, the Portal Server must download Linux components to *each-end user desktop* before any streams will play. This should only be performed by a system administrator. When you access the Portal Server for the first time, you will see a message in the embedded player window indicating that the appropriate plugins are not installed. See "Installing Linux Components" in the *Portal Server Release Notes* for detailed instructions. On Linux PCs, Portal Server functionality is the same as in Windows except that the **Add Video** feature is not available. Table 4 shows the stream types supported for each environment; Table 5 shows the operating systems that are tested and supported. Note that there are certain performance limitations in Linux environments; see the *ETV Portal Server Release Notes* for information and recommendations.

Table 4. Supported Stream Types – Macintosh and Linux

Environment	Supported Streams	Closed Captions
Macintosh	Safari – MPEG-1, MPEG-2, MPEG-4, WM.	Supported for MPEG-1/MPEG-2 streams, and for MPEG-4 and WM with VBrick plugin.
	Firefox – MPEG-1, MPEG-2, MPEG-4, WM.	Supported for MPEG-1/MPEG-2 streams, and for MPEG-4 and WM with VBrick plugin.
Linux	Firefox – MPEG-1, MPEG-2, MPEG-4, WM.	Supported for MPEG-1, MPEG-2, MPEG-4, and WM streams.

Table 5. Supported Operating Systems and Browsers – Macintosh and Linux

Operating System	Browser †
Mac OS X 10.3 (Panther)	Safari 1.2, Firefox 1.0
Mac OS X 10.4 (Tiger)	Safari 2.0, Firefox 1.0
Mac OS X 10.5 (Leopard)	Safari 3.0, Firefox 1.0
Linux Red Hat 9.0	Firefox 1.0
Linux Fedora Core 3	Firefox 1.0
Linux Fedora Core 4	Firefox 1.0

† Use version shown or higher.

Port Requirements

The drawing below, and the table that follows, show the required port configuration for various Portal Server devices. *All ports in the drawing are TCP except as noted.*

© 2007 VBrick Systems, Inc.

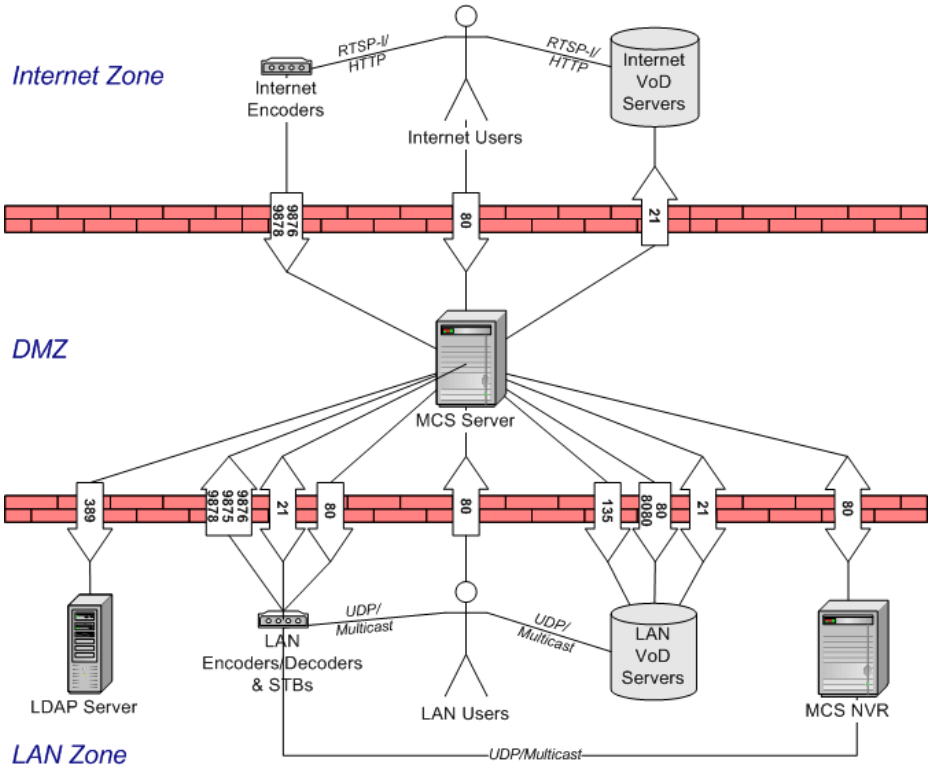


Table 6. Port Requirements†

Zone	Port(s)	Protocol	Description
Internet > DMZ	80	TCP	Web request from client to MCS.
Internet > DMZ	9876/9878	UDP	Management/RTSP SAP announce from VBrick to MCS.
DMZ > Internet	21	TCP	FTP from MCS to VOD Server (Darwin/Windows Media/ FTP).
LAN > DMZ	80	TCP	Web request from client to MCS.
LAN > DMZ	9875/9876/ 9878	UDP	Multicast/Management/RTSP SAP announce from VBrick to MCS.
LAN > DMZ	21	TCP	FTP from VBStar to MCS (auto-FTP to MCS autoingest directory).
DMZ > LAN	21	TCP	FTP from MCS to VBStar (content discovery).
DMZ > LAN	80	TCP	Management command from MCS to VBrick/STB.
DMZ > LAN	80/8080	TCP	Web service request from MCS to VOD Server (VOD-W/ NXG).
DMZ > LAN	21	TCP	FTP from MCS to VOD Server (Darwin/Windows Media/ FTP).
LAN > DMZ	21	TCP	FTP from VOD Server (NXG/VOD-W) to MCS.

Zone	Port(s)	Protocol	Description
DMZ > LAN	135	TCP	Management command from MCS to Windows Media (DCOM).
DMZ > LAN	80	TCP	Web service request from MCS to Network Video Recorder.
DMZ > LAN	80	TCP	Web service request from Network Video Recorder to MCS.
DMZ > LAN	389	TCP	LDAP lookup from MCS to LDAP Server (e.g. Active Directory).

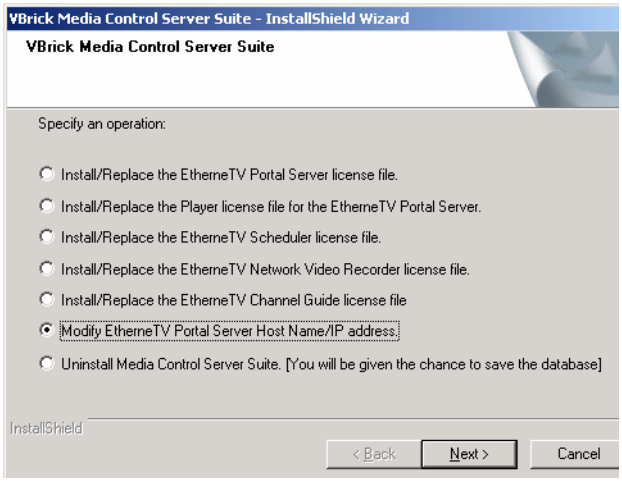
† All ports are TCP except as noted.

Portal Server License Files

You are prompted to install a license (`.lic`) file as part of the ETV Portal Server installation process. Different Portal Server functionality is available depending on the type of license you purchase and install. (For example if you do not install a Scheduler license, you will not see a **Scheduled Programs**, as shown above, option in the Portal Server client application.) After initial installation you can install a different license as necessary by using **Add or Remove Programs**.

▼ To install or modify a Portal Server license file:

1. Go to **Start > Control Panel > Add or Remove Programs > VBrick Media Control Server Suite**.
2. Click **Change/Remove** and select the appropriate license file type (see below).
3. Click **Next**, then browse to the file and click **Open**.
4. When done, manually close the window and launch the application. There is no need to restart the host machine.


VBrick Media Control Server Suite - InstallShield Wizard
VBrick Media Control Server Suite
Specify an operation:
Install/Replace the EtherneTV Portal Server license file.
Install/Replace the Player license file for the EtherneTV Portal Server.
Install/Replace the EtherneTV Scheduler license file.
Install/Replace the EtherneTV Network Video Recorder license file.
Install/Replace the EtherneTV Channel Guide license file
Modify EtherneTV Portal Server Host Name/IP address.
Uninstall Media Control Server Suite. [You will be given the chance to save the database]
InstallShield
< Back
Next >
Cancel

© 2007 VBrick Systems, Inc.

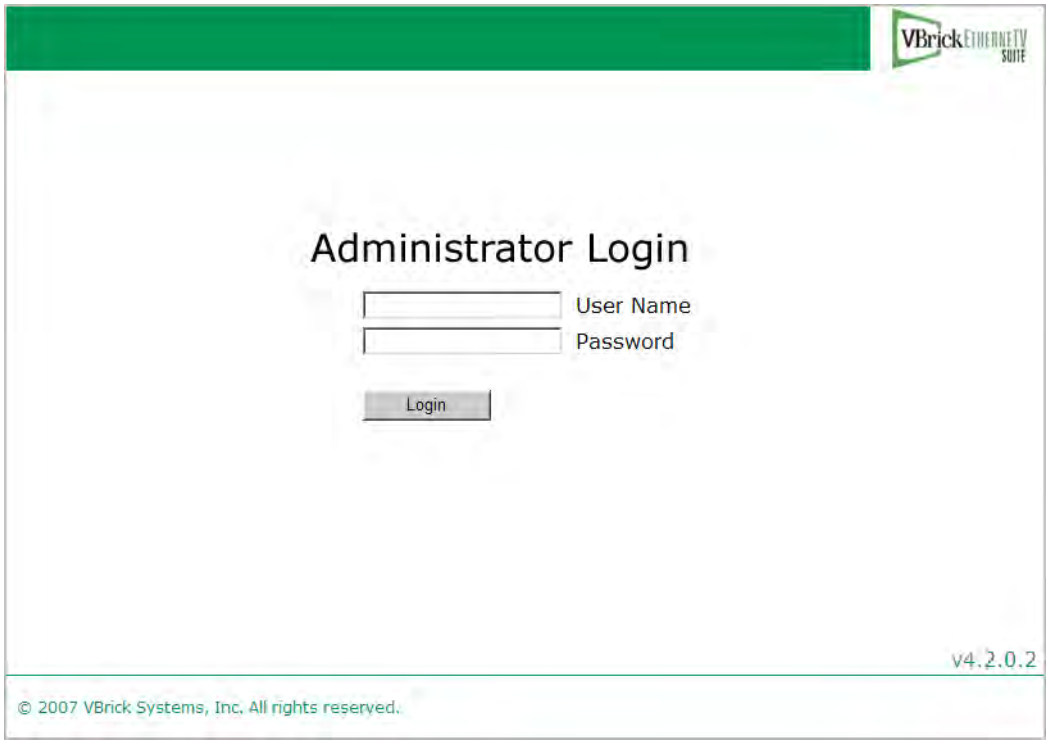
Table 7. Portal Server License Files

License File	Description	License Errors
Player	The embedded Windows Media Player has restrictions on the number of licensed users. Use this option to select a license file that modifies the number of allowed users for various MPEG-1, MPEG-2, and MPEG-4 streams.	If not installed, popup message displayed when you try to launch a stream.
Scheduler	Enables the broadcast or recording of future events. See the *ETV Portal Server User Guide* for more information.	If not installed, the Add option will not be shown on Scheduler page.
Network Video Recorder	A Network Video Recorder is a standalone recorder option that can speed up recording operations and/or enhance Portal Server performance. (See ETV Network Video Recorder on page 8.)	If not installed, there will be a "record" failure for more than two concurrent record requests.
Channel Guide Server	Enables access to the Channel Guide Server for TV Stations that are typically provided by a third-part content provider.	If not installed, there will be no TV Stations or access to the Channel Guide server.
Modify Host Name or IP Address	Lets you auto-detect or manually change the Portal Server Host Name. This name must match the machine name on which ETV Portal Server is installed. If you change the host machine name, use this option to change the Portal Server Host Name.	Not applicable.
Uninstall Media Control Server Suite	Remove all ETV Portal Server components. You are prompted to save the database as desired.	Not applicable.

Admin Console Login

The ETV Portal Server can be administered from Windows-based PCs using Internet Explorer 6.0 or higher only. The Admin Console pages are best viewed at 1024x768 resolution. The Admin Console is not supported on Macintoshes or Set Top Boxes, or with Firefox or other browsers. In order to access the administrative functions enter the following address in the Internet Explorer browser of the PC where `myserveraddress` is the host name or IP address of the ETV Portal Server. The session will timeout after 20 minutes of inactivity. `admin` is both the default user name and password.

`http://myserveraddress/admin/`



Note As a standard best practice, VBrick recommends changing the default administrator User Name and Password. Go to **Global Settings > Global Assignments** on the Admin Console.

Admin Console Options

Login to the ETV Portal Server Admin pages with a valid user name and password to display the following window. This window provides access to all admin configuration options.

© 2007 VBrick Systems, Inc.

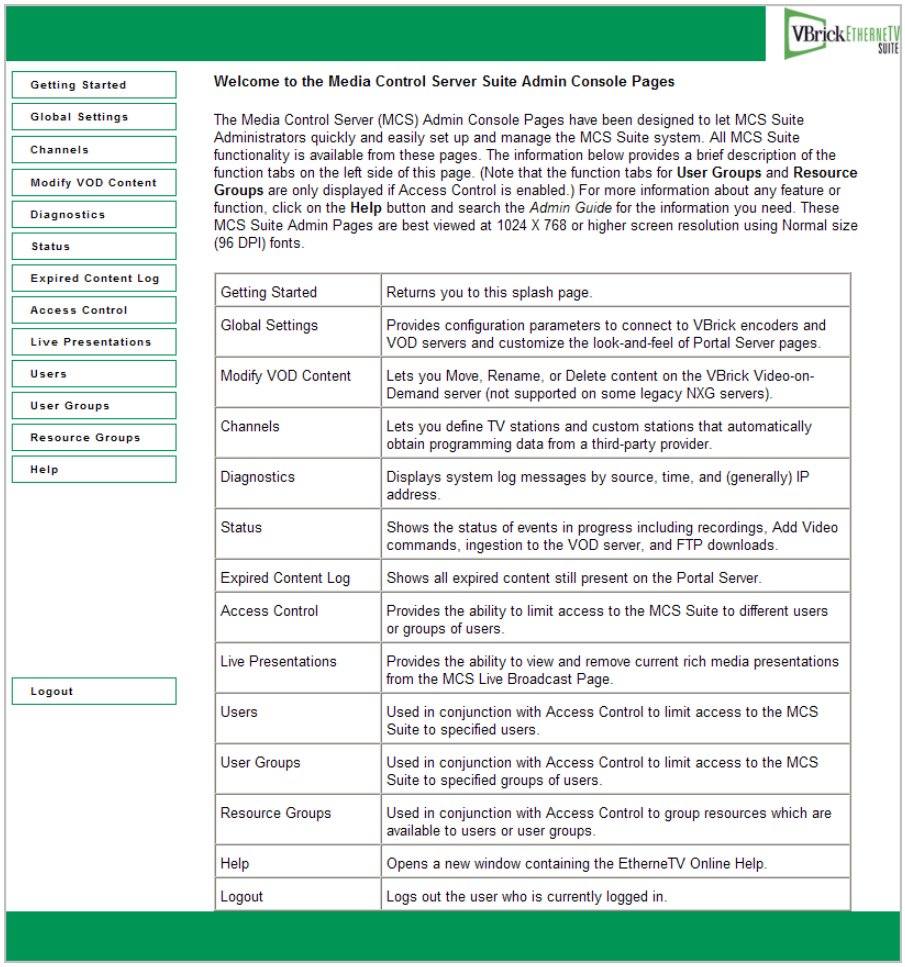

Getting Started
Global Settings
Channels
Modify VOD Content
Diagnostics
Status
Expired Content Log
Access Control
Live Presentations
Users
User Groups
Resource Groups
Help
Logout
Welcome to the Media Control Server Suite Admin Console Pages
The Media Control Server (MCS) Admin Console Pages have been designed to let MCS Suite Administrators quickly and easily set up and manage the MCS Suite system. All MCS Suite functionality is available from these pages. The information below provides a brief description of the function tabs on the left side of this page. (Note that the function tabs for User Groups and Resource Groups are only displayed if Access Control is enabled.) For more information about any feature or function, click on the Help button and search the Admin Guide for the information you need. These MCS Suite Admin Pages are best viewed at 1024 X 768 or higher screen resolution using Normal size (96 DPI) fonts.
Getting Started | Returns you to this splash page.
Global Settings | Provides configuration parameters to connect to VBrick encoders and VOD servers and customize the look-and-feel of Portal Server pages.
Modify VOD Content | Lets you Move, Rename, or Delete content on the VBrick Video-on-Demand server (not supported on some legacy NXG servers).
Channels | Lets you define TV stations and custom stations that automatically obtain programming data from a third-party provider.
Diagnostics | Displays system log messages by source, time, and (generally) IP address.
Status | Shows the status of events in progress including recordings, Add Video commands, ingestion to the VOD server, and FTP downloads.
Expired Content Log | Shows all expired content still present on the Portal Server.
Access Control | Provides the ability to limit access to the MCS Suite to different users or groups of users.
Live Presentations | Provides the ability to view and remove current rich media presentations from the MCS Live Broadcast Page.
Users | Used in conjunction with Access Control to limit access to the MCS Suite to specified users.
User Groups | Used in conjunction with Access Control to limit access to the MCS Suite to specified groups of users.
Resource Groups | Used in conjunction with Access Control to group resources which are available to users or user groups.
Help | Opens a new window containing the EtherneTV Online Help.
Logout | Logs out the user who is currently logged in.

Table 8. Admin Options

Option	Description
Getting Started	The ETV Portal Server splash page shown above.
Global Settings	Provides system-wide configuration parameters to connect to VBrick encoders and VOD servers as well as to customize the look of the ETV Portal Server pages.
Channels	Lets you define TV stations and custom stations that obtain programming data from a third-party provider.
Modify VOD Content	Provides the ability to Move, Rename, or Delete assets on the EtherneTV-VOD Video-on-Demand server. (Not supported on some legacy NXG servers.)
Diagnostics	Displays system log messages by source, time, and (generally) IP address.
Status	Shows the status of events in progress including recordings, Add Video commands, ingestion to the VOD server, and FTP downloads.
Expired Content Log	Shows all expired content still present on the Portal Server. Use Purge All to delete unwanted content.

Option	Description
Access Control	Provides the ability to limit access to the ETV Portal Server system to different users or groups of users.
Live Presentations	Provides the ability to view and remove current live presentations from the Live Broadcasts page.
Users†	Used in conjunction with Access Control to limit access to the ETV Portal Server system to different users.
User Groups†	Used in conjunction with Access Control to limit access to the ETV Portal Server system to different groups of users.
Resource Groups†	Used in conjunction with Access Control to group resources which can then be provided to users or user groups.
Help	Displays the ETV Portal Server online help system in a new window.
Logout	Logs out the user who is currently logged in.

† Users, User Groups, and Resource Groups are only displayed if Access Control is enabled. See Users and User Groups on page 87 for a description of these functions.

Internet Explorer 7.0 Configuration

The Admin Console and the Portal Server user interface support the browsers shown in Table 3 and in Table 5. When using Internet Explorer 7.0, there are additional security settings required for compatibility with the Portal Server.

▼ To configure the Portal Server for Internet Explorer 7.0:

1. Go to **Tools > Internet Options > Security** and select **Custom level**.
2. Under **Active X controls and plugins** set the following parameters:
   - **Allow previously unused ActiveX controls to run without prompt** – Enable
   - **Automatic prompting for ActiveX controls** – Disable
   - **Display video and animation on a webpage that does not use external media player** – Enable
   - **Download signed ActiveX controls** – Prompt
   - **Run ActiveX controls and plug-ins** – Enable
   - **Script ActiveX controls marked as safe for scripting** – Enable

© 2007 VBrick Systems, Inc.

Chapter 2

Global Settings

Global Settings include configuration settings and parameters that apply to the entire system. Global Settings include all of the following.

Topics in this chapter

Global Assignments 19
Custom Fields 25
Stream Restrictions 26
Servers 27
VBricks 36
Control Devices 38
Set Top Boxes 44
Recorders 46
Script Devices 48
Scripts 49
URLs 52
Emergency Broadcast 55
Program Names 59
Manage Playlists 60
Access Logging 61

Global Assignments

Global Assignment are listed below. Most are self-explanatory and consist of text boxes where you enter appropriate values.

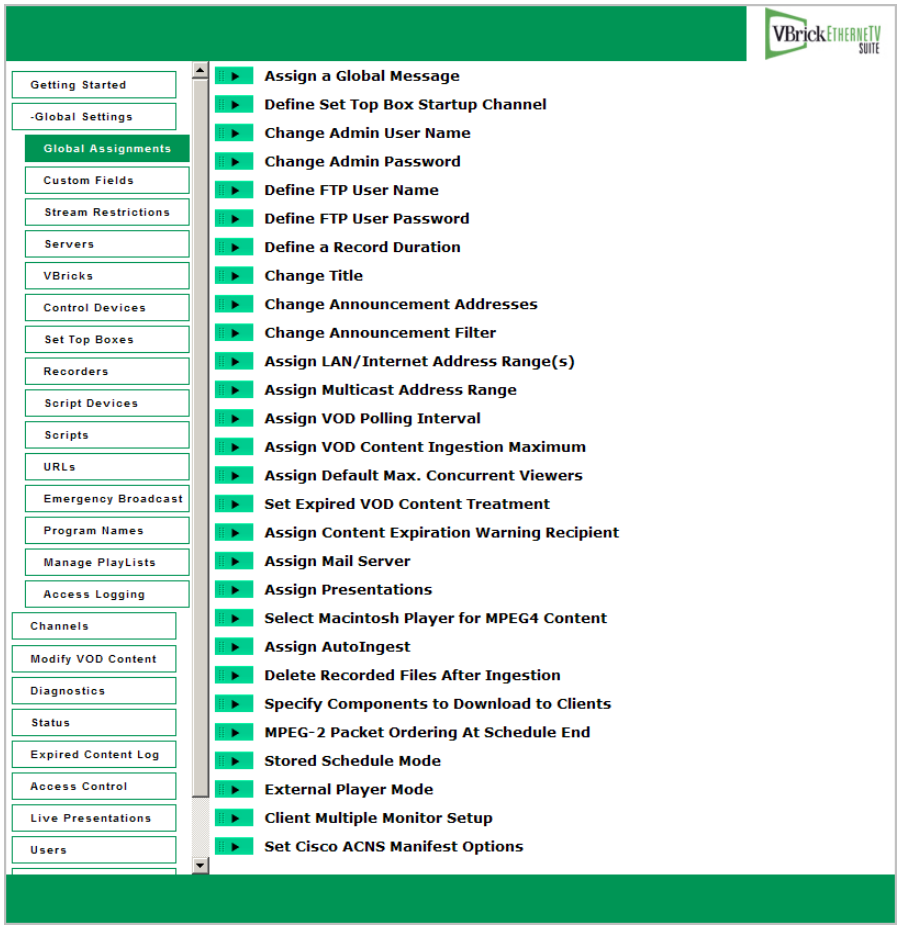


Table 9. Global Assignments

Item	Description
Assign a Global Message	The global message will be displayed in the message area of the Portal Server user interface when there is no program information available. Enter the message text and click Submit. Example: *There will be an all hands meeting today at 4:00 PM in the boardroom.* Note that if you are running the Portal Server on a Set Top Box, the message area will not display more than 4 lines of text.
Define Set Top Box Startup Channel	When an STB (in ETV Portal Server Start mode) accesses the **Watch live broadcasts** page, it can be set to automatically play a defined channel in the Preview Window. Highlight that channel from the list and click Submit. If there are no channels listed, channels must first be defined as Customized Live Streams.
Change Admin User Name	Change the default admin user name of `admin`. Use any combination of alphanumeric and special characters *except* slashes, quotes, or commas.

© 2007 VBrick Systems, Inc.

Item	Description
Change Admin Password	Change the default admin password of `admin`. Use any combination of alphanumeric and special characters *except* slashes, quotes, or commas.
Define FTP User Name	ETV Portal Server is defaulted for "anonymous" FTP access which is configured in Windows IIS Default FTP Site. If a more secure FTP access is desired, the User Name can be changed in IIS (see the Windows Server documentation for details). The same User Name should be entered here. Use any combination of alphanumeric and special characters *except* slashes, quotes, or commas. If configuring for VBPresenter, see Configuring an FTP User on page 114.
Define FTP User Password	ETV Portal Server is defaulted for "anonymous" FTP access which is configured in Windows IIS Default FTP Site. If a more secure FTP access is desired, the Password can be changed in IIS (see the Windows Server documentation for details). The same Password should be entered here. Use any combination of alphanumeric and special characters *except* slashes, quotes, or commas. If configuring for VBPresenter, see Configuring an FTP User on page 114.
Define a Record Duration	Applies to the on-demand **Record** pushbutton only (not to scheduled recording). Defines the maximum duration (default 120 minutes) allowed for a continuous recording. Maximum record duration limited only by size of hard drive.
Change Title	Changes the text (i.e. VBrick Systems) that is displayed on the upper left hand corner of the Portal Server User Interface. To leave blank, enter at least one space. Note that the title text is white and cannot be changed.
Change Announcement Addresses	*Changing these from the defaults is highly discouraged and should only be done if advised by a VBrick technician or Network Administrator.* Changes the Management, Multicast, and RTSP addresses on which Announcements (SAPs) are received. By default all VBrick devices are set to the same addresses and ports as the defaults in ETV Portal Server. These have to match on all devices for proper functionality.
Change Announcement Filter	Filters SAP announcements so that only the specified IP addresses are shown on the Live Broadcasts page in ETV Portal Server. Wildcards are allowed. For example 255.*.*.* displays only those addresses in the range 255.0.0.0 – 255.255.255.255.

Item	Description
Assign LAN/Internet Address Range(s)	Define the range(s) of IP addresses that define the LAN or the Internet domain. Any IP addresses outside the range are assumed to be from the domain you did *not* select. Check one option and, if necessary, use the text box to enter the range(s) separated by a comma, a semicolon, or a new line. For details, see ETV Internet-Based Servers on page 7. • All Users, Servers, and VBricks are in the LAN Domain (default). • All Users, Servers, and VBricks are in the Internet Domain. • Specify LAN Address Range(s); assume users/servers/ VBricks outside this range(s) are in the Internet domain. • Specify Internet Address Range(s); assume users/servers/ VBricks outside this range(s) are in the LAN domain. • Always use TCP protocol (HTTP Tunneling/RTSP Interleaving) for MPEG-4 and Windows Media content – Use only with Internet-compatible (VOD-D, VOD-W, and VOD-WM) servers. If checked, the Portal Server will always use HTTP tunneling or RTSP interleaving using the **HTTP Tunneling Port** defined for the server (see Add/ Modify VOD/FTP Servers on page 28). **Note**: Standard VBrick Set Top Boxes do not support HTTP tunneling and will not play MPEG-4 content if this option is selected.
Assign Multicast Address Range	Defines the current multicast IP address range and port range. The default multicast IP range is 225.1.1.0– 239.128.255.255. The default port range is 1040–65534.
Assign VOD Polling Interval	Not generally changed. Defines the interval at which the Portal Server polls the VOD server(s) for new content (default 120 minutes). This is only used to poll for content added to the VOD from an interface *other than ETV Portal Server*. When adding a server, use Sync Now to sync the program listings on the client Browse Video Library page with the content on the new server.
Assign VoD Content Ingestion Maximum	Defines the maximum number of simultaneous video files that can be ingested to the VOD Video-on-Demand server. The default is set to 2. Increasing the default may increase the speed at which files will be transferred to the VOD server, but may result in playback issues from the Video-on-Demand server. VBrick recommends keeping the default of 2 for all supported VOD servers.
Assign Default Max. Concurrent Viewers	Defines the *default* maximum concurrent viewers allowed for new live or stored (VOD) content. An entry on the **Stream Restrictions** page or the **Modify VOD Content** page will override these value for live and stored streams respectively.

© 2007 VBrick Systems, Inc.

Item	Description
Set Expired VOD Content Treatment	Specifies whether expired content will be kept or automatically deleted at the expiration date.
Assign Content Expiration Warning Recipient	Enter one e-mail address for the person who is responsible for renewing copyrighted or otherwise protected content. When you configure or change either the recipient or the mail server, the Portal Server will attempt to send a test message. Check that this message is successfully delivered. The Portal Server validates the e-mail address but cannot detect other mail delivery failures. If the user's mail box is full, for example, the message will not reach its intended recipient to warn of impending content expiration. For more about content expiration, see Copyright Protection on page 3.
Assign Mail Server	Required field. SMTP mail server name. In Microsoft Exchange, for example, go to Tools > E-mail Accounts > E-mail > Microsoft Exchange Server > servername. An e-mail to the assigned Content Expiration Warning Recipient is generated when you configure or change this field.

Assign Presentations	VBPresenter is used to create multimedia presentations that can be launched from the Portal Server. The **Current Presentations Directory** defines the virtual directory on the Portal Server where the live presentations are stored—the default is `Presentations`. During a new Portal Server installation, the required virtual and physical directories are automatically created. To use a different virtual directory, create the virtual directory in IIS and enter only the virtual directory name in this field—*do not enter the complete path*. The **Current Presentations User** is a pseudo VBPresenter user who will be given permission to publish to specified directories and VOD servers. Configuring a Presentation User on page 114 explains how to create this user; contact VBrick Support Services if you need help.
	
	If you are upgrading from Portal Server v4.0.1 or earlier and using VBPresenter, you will need to manually create two virtual directories (`Presentations` for live presentations and `MCSPresentations` for stored presentations), giving the user `Everyone` full permissions, and mapping the local paths respectively to:
	`C:\Program Files\VBrick\MCS\Presentations`
	`C:\Program Files\VBrick\MCS\MCSPresentations`

Select Macintosh Player for MPEG4 Content	Select the player to use for MPEG-4 content on Macintosh clients: • VBrick Player – users will be prompted to install a VBrick plugin the first time they launch MPEG-4 content. • Apple QuickTime Player – no plugin required. Does not support access logging.

Item	Description
Assign AutoIngest	The current autoingest via XML user name that has access and publishing rights to a VOD server. See AutoIngest Content via XML on page 121 for more information.
Delete Recorded Files After Ingestion	Used with scheduled recording and push button recording. Specifies whether or not to delete the recorded file from the NVR after ingestion. Enabled by default.
Specify Components to Download to Clients	This setting defines whether the Portal Server will download additional components to client machines when the client first makes contact with the Portal Server—before any streams or assets are selected for playback (see Download Components on page 10 for more information.) *Any changes to these settings apply to new client machines only and will not affect previously configured machines*. The settings here apply to Internet and/or LAN users as defined in the **Assign LAN/Internet Address Range(s)** in Global Assignments (see above). The default is to download all components to all clients. For Windows clients you can selectively choose any combination of settings; for Macintosh or Linux clients, any one selection will download all components for all clients. • MPEG-1 Video Support – makes MPEG-1 files playable. • MPEG-2/1 Video Support – makes both MPEG-2 and MPEG-1 files playable. • MPEG-4 – makes MPEG-4 files playable. • WM Video Support for Firefox on Windows PC – makes Windows Media files playable on Firefox. • 'Add Video' Utility – enables or disables the "add video" functionality on client machines.
MPEG-2 Packet Ordering at Schedule End	Network hardware infrastructure determines the order in which packets arrive at a destination. To improve video quality, VBrick MPEG-2 appliances reorder packets by default. Since this reordering can cause an increase in latency and affect applications like video conferencing, you can set packet ordering to disabled at schedule end.
Stored Schedule Mode	Used when creating a live broadcast schedule for stored content. Note that the following parameters are "sticky." They remain associated with the schedule even if the Stored Schedule Mode is subsequently changed. • Content Centric – content titles are shown; content servers are not shown. The content is downloaded from load-balanced servers. • Server Centric – content servers are shown with a tree control for selecting content. The content is downloaded from a specific server and is not load balanced.

© 2007 VBrick Systems, Inc.

Item	Description
External Player Mode	Windows only. Determines whether or not multiple streams can be displayed by launching external player windows. Default = Single. You can launch multiple windows but you can only record one stream at a time.
Client Multiple Monitor Setup	The Portal Server supports dual client monitors. However, if you experience problems when using a second monitor, disable the DirectX component VMR9.
Set Cisco ACNS Manifest Options	Check the box to enable generation of a Cisco ACNS Manifest File. (The Cisco ACNS server must be configured to point to this file.) Select the files (MPEG-4 and/or WM) to include in the file, and specify a Manifest Generation Interval (default = 10 minutes) that defines how often the file will be regenerated. Click Generate Now to create an "on demand" file. ACNS copies all MPEG-2 and WM video files to all (Windows Media, Darwin, and VOD-W) servers in your EtherneTV system. Additional configuration steps are required on the VOD-W server only. See ACNS Configuration on page 133 for more about ACNS.

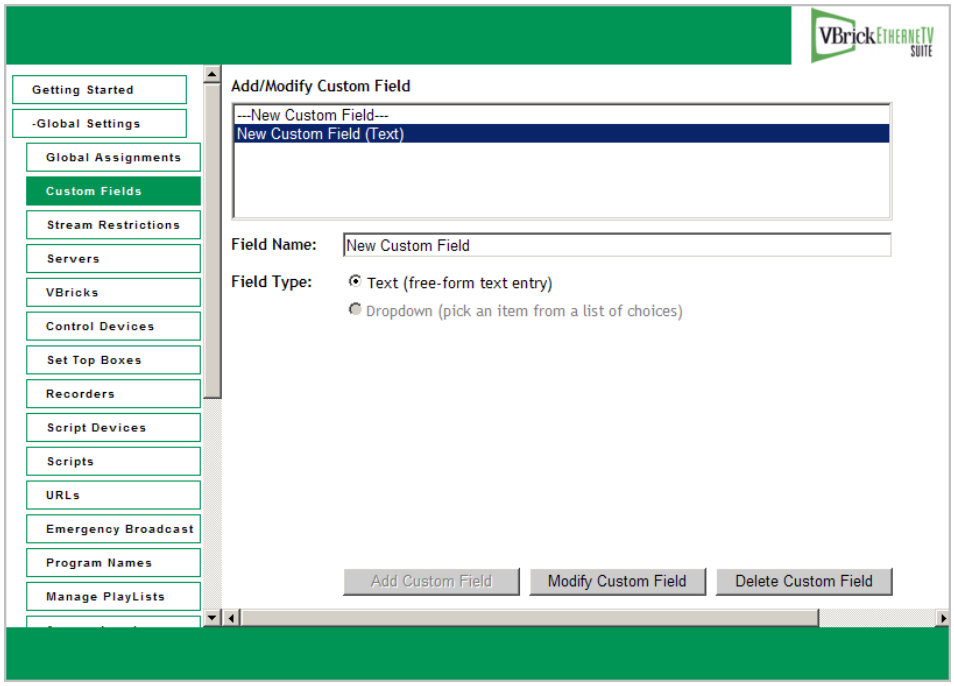
Custom Fields

Custom fields are used to add additional fields to the Info pages associated with stored videos and live broadcast streams. All stored videos, and those live streams that have been "customized," have an **Info** hyperlink. By default, the Info page has fields for **Description** and **Keywords**. The Custom Fields functionality lets you add additional "custom" fields that are appropriate to your business or application. This lets you provide more information on the page and it also makes it easier to search for specific streams. (All defined fields are listed in the dropdown list box next to the **Search** button.)

When you add a custom field using this function, the field is available to administrators as a selection in the **Customize Streams** window. It is also available to end users as the **Modify Info** button on the Info pages associated with stored videos (if they have content publishing permissions).

▼ To create a Custom Field:

1. Go to **Global Settings > Custom Fields**.



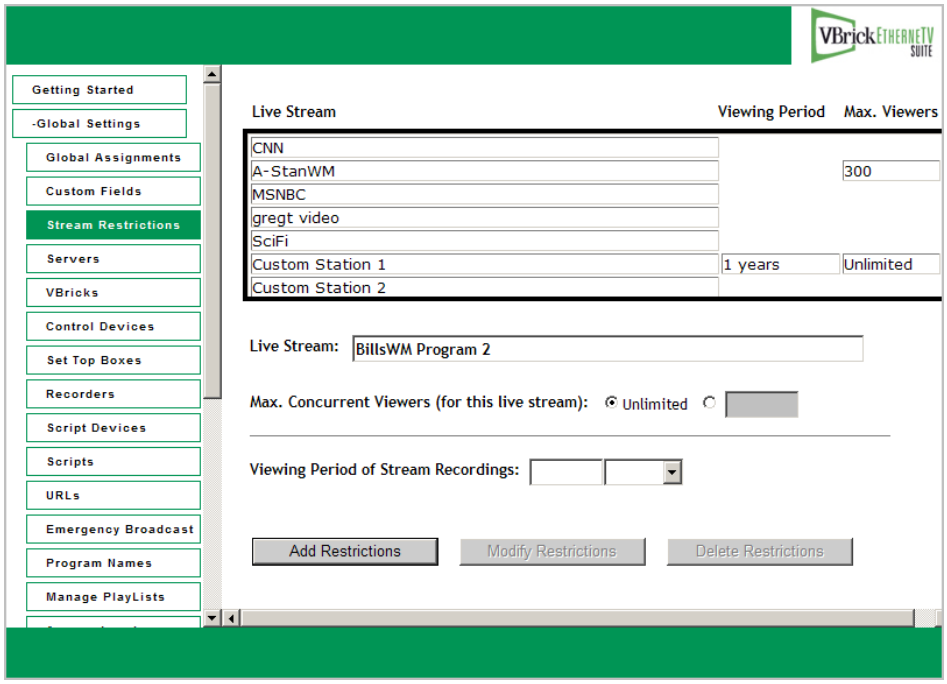
2. Enter a **Field Name** and a **Field Type**. If you select **Dropdown**, you can add items one at a time followed by **Add Item**. These items will populate a dropdown list box on the **Customize Streams** page.
3. When done, click **Add Custom Field**. The field will be added to the panel at the top of the window; it will also be available as an option when you are customizing a stream.

Add/Modify Custom Field	This panel shows the existing custom fields that have previously been defined.
Field Name	The field name you want to display on the Info page for this stream or video.
Field Type	This determines how the field will be displayed on the **Customize Streams** page, either as a text field or as a dropdown list box.

Stream Restrictions

Use this page to set and the viewing period for live stream recordings and the maximum number of concurrent viewers. There are no default expiration dates for live streams when a recording is made but administrators can automatically set the content from a specific stream to expire by setting a viewing period. For more about content expiration see Copyright Protection on page 3.

© 2007 VBrick Systems, Inc.



Live Stream	Click on any live stream shown in the list to populate this field.
Max. Concurrent Viewers	Set the maximum number of concurrent viewers for this stream to unlimited or any number greater than zero.
Viewing Period of Stream Recordings	Set the length of the viewing period for a file recorded with this stream in hours, days, weeks, months, or years. The file will no longer be available for viewing at the end of the period and will be deleted or saved as configured in Global Assignments > Set Expired VOD Content Treatment.

Servers

Use the **Servers** page to add or modify VOD or FTP servers, or to add or modify VOD Content Folders. Note that you can cluster multiple servers to increase throughput: the ETV Portal Server will automatically load balance all servers defined on the **Servers** page; no additional configuration is necessary. Note that content added by users in the Internet zone will only be ingested to VOD servers in the Internet zone for which they have permissions. Content added by users in the LAN zone will be ingested to all VOD servers to which they have permissions. See ETV Video-on-Demand Servers on page 6 for more about ETV servers.

Note It may take up to 20 minutes for new server content to be displayed in the ETV Portal Server. To make content available immediately, go to **Global Settings > Global Assignments > Assign VOD Polling Interval** and click **Sync Now**.

Using Secure FTP

In v4.2 or higher, VBrick's FTP client supports secure FTP connections from the end user (client), Portal Server and NVR to the VOD servers. This is accomplished using FTP over SSL (FTPS protocol). Having a client that supports FTPS however, is not enough to have

secure FTP connections throughout the system. The FTP servers on all VOD servers also need to support FTPS for a secure connection to exist. If a secure connection cannot be established, the client will revert to the standard FTP protocol. The FTP server on Windows platforms (IIS) does not currently support FTPS. *Therefore, to have secure connections, you must install a third-party add-in on all Windows VOD servers.* Of the various solutions available, VBrick recommends FTP Guardian. FTP Guardian is a wrapper for IIS that serves as a proxy between a secure client and an unsecured IIS. You change the FTP port of IIS to an arbitrary port (10021 for example), then you start the FTP Guardian service. It binds to port 21 and all incoming FTP clients communicate using a secure front that proxies the calls to IIS on port 10021. Be aware that this add-on, for Windows servers only, is not sold or supported by VBrick. It requires a server wrapper and additional .dlls.

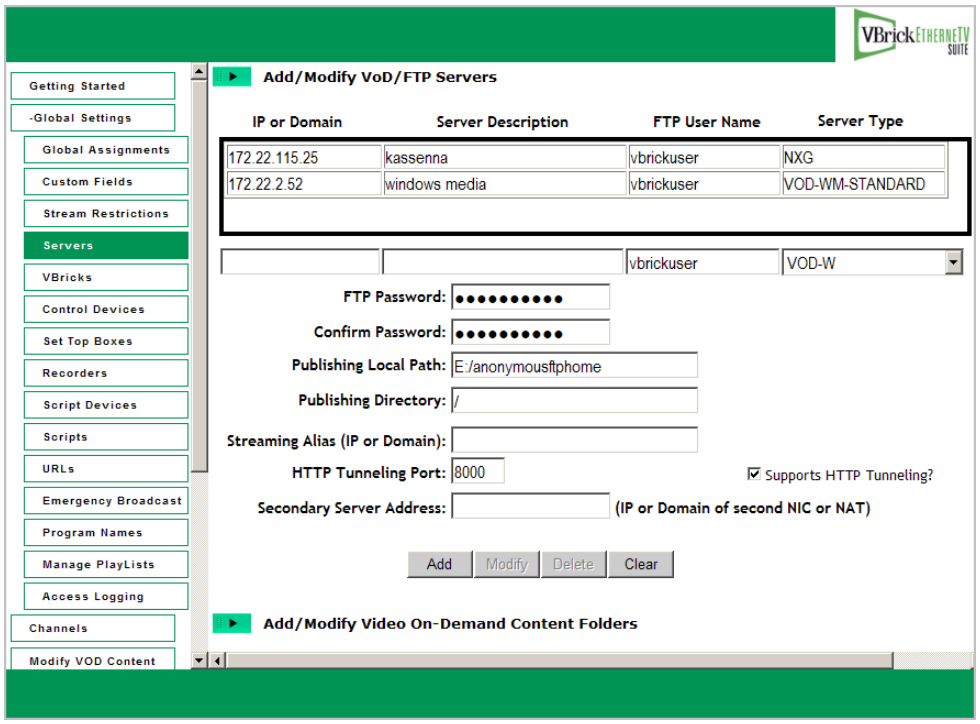
▼ To install FTP Guardian:

1. Go to http://www.tcpdata.com/ftpg_license.shtml
2. Click and run **Download ftp Guardian Server Wrapper - 600K** on the VOD server.
3. Click **Download SSL Libraries - 380K** on the VOD server.
4. Then open the .zip file and copy `libeay32.dll` and `ssleay32.dll` into `C:\Program Files\ftpgs`

Add/Modify VOD/FTP Servers

Use this window to add Video-On-Demand Server(s) to the ETV Portal Server. If the network supports Windows 98 users, you *must* use the IP address of the VOD server—not the host name. After selecting a **Server Type** VBrick recommends you keep the default settings for FTP Password, Publishing Local Path, Publishing Directory, etc. unless there is a compelling reason to change them. Nor is it necessary to create a Streaming Alias. Leave this parameter blank unless you are using HTTP Tunneling.

Adding NXG, VOD-W, and VOD-D Servers



© 2007 VBrick Systems, Inc.

Figure 4. Add VOD-W Server

IP or Domain	This is the primary IP address or Host Name of the VOD server for LAN users (see also **Secondary Server Address** below). The Server Name or IP address entered into the ETV Portal Server must be accessible by the ETV Portal Server. (If the network supports Windows 98 users, you *must* use the IP address.)
Server Description	This allows the administrator to define a descriptor such as location.
FTP User Name	This is the FTP user name that the Portal Server uses when publishing content to the server. The default user name for NXG, VOD-D, VOD-WM, and FTP servers is `vbrickuser`. The default user name for VOD-W servers is `anonymous`. The FTP User Name refers to a user account that already exists on the server. If the FTP User Name is changed on any VOD server, it must be changed here as well. Use any combination of alphanumeric and special characters.
Server Type	• NXG – Linux-based Kasenna VOD server. • VOD-W – Windows-based InfoValue VOD server. • VOD-D – Darwin Open Source server for Linux, Windows, Mac, etc. Ingests and plays MPEG4 content only. Requires an FTP server. See Creating a VOD-D FTP Server on page 34. • VOD-WM-Standard – Microsoft Windows Media Server (unicast only). Requires an FTP server. See Creating a VOD-WM FTP Server on page 33. • VOD-WM-Enterprise – Microsoft Windows Media Server (unicast or multicast). Requires an FTP server. See Creating a VOD-WM FTP Server on page 33. • FTP – Use FTP only if you want to copy from the Recorder server to another FTP server in which case it records to `ftp:\root`.
FTP Password	The FTP password the Portal Server uses when publishing content to the server. The default FTP password for NXG, VOD-D, VOD-WM, and FTP servers is `vbrickuser`. The default FTP password for VOD-W servers is `anonymous`. If the FTP Password is changed on the server, it must be changed here as well. Use any combination of alphanumeric and special characters.
Publishing Local Path	Maps the Publishing Directory to the physical location on the VOD server.
Publishing Directory	Used for Add Video, FTP, or Record. The logical path to a folder under `FTP` root. This is the staging area on the VOD server from which files are ingested to the destination folder.
Streaming Alias (IP or Domain)	Some content hosts (PowerStream, Akamai, etc.) use one host name for FTPing and indexing content, and another host name for streaming content. If necessary, use this field to identify the host name alias for streaming content.

HTTP Tunneling Port	*VOD-WM and VOD-D only.* VOD-WM and VOD-D servers can stream to clients via the HTTP protocol. By default this uses port 80. If another process on the server (for example a web server) is also using the HTTP protocol, there will be a conflict on this port. This setting lets you select a different port (1–65535 with limitations) to be used when streaming via HTTP. This setting *must* correspond with the port setting on the server. See "Assign LAN/ Internet Address Range > Always use TCP protocol for MPEG-4 content" in Global Assignments on page 19.
Supports HTTP Tunneling?	*VOD-W only.* Determines whether or not the server supports HTTP tunneling. Default = checked. Go to Global Assignments to actually enable HTTP tunneling. See "Assign LAN/Internet Address Range > Always use TCP protocol for MPEG-4 content" in Global Assignments on page 19. Uncheck if you are using a VOD-W server installed *before* Portal Server v4.2.
Secondary Server Address	A VOD server can have two addresses: one for Internet users and one for LAN users (see also **IP or Domain** name above). This is the secondary server address for Internet users. It is the IP address or domain name of a second NIC or a NAT.
Enable URL Password Protection	*VOD-W only.* Default = unchecked. To enable URL password protection, check the box and enter and confirm a password. The default password = `vbrickkey`. If checked, all video requests sent to VOD-W servers by the ETV Portal Server will have a security token embedded in the URL. The VOD-W server will validate and deny the request if the token is absent or invalid.

Adding WM Servers

Although the VOD-WM Enterprise server supports numerous multicast types, the Portal Server creates and displays only "File" multicasts which stream a single file. A Windows Media server administrator can create other multicast types using the Windows Media Services interface but these multicast types are not supported and may not be displayed in the Asset Library.

© 2007 VBrick Systems, Inc.

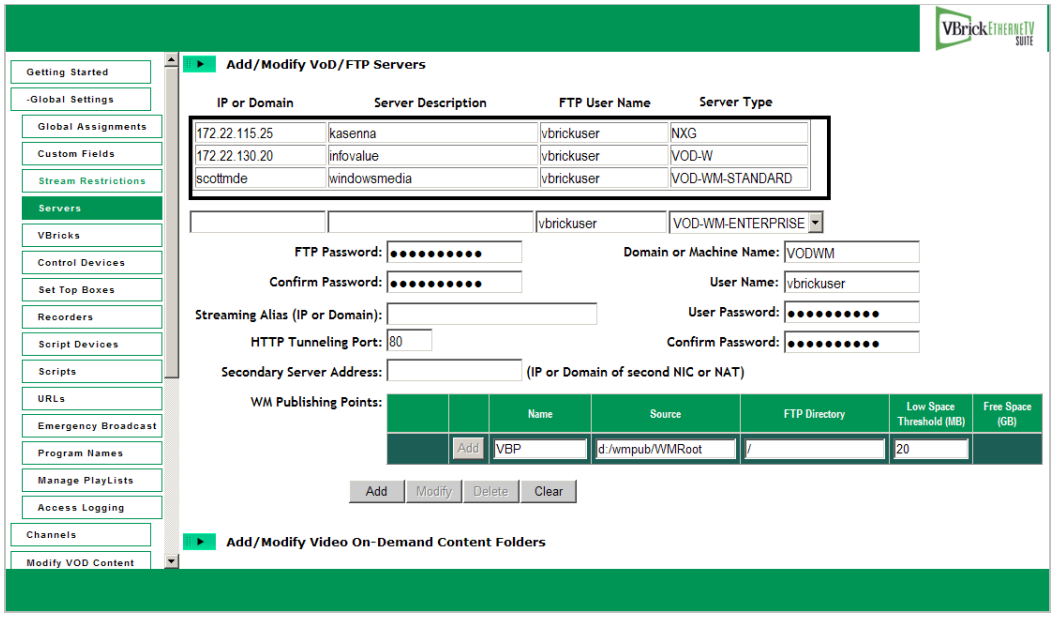


Figure 5. Add VOD-WM Server

Domain or Machine Name	When the ETV Portal Server and the VOD-WM server reside in the same domain, this is the name of that domain. When workgroups are being used, this is the machine name of the VOD-WM server. Note: the machine name is *not* the IP address of the server.
User Name	The name of a valid user that has administration privileges on the VOD-WM server or the network domain. If the VOD-WM Server is within a domain, the name entered here will be a domain user. That domain user must have administration privileges on the VOD-WM Server. If the VOD-WM Server is part of a workgroup, the name entered here will be a local user with administration privileges on the VOD-WM Server. A local user with administrator privileges having the same name must also exist on the MCS Portal Server. Note: The MCS Portal Server and VOD-WM Server(s) must all be within a domain or part of a workgroup. Any topology that mixes servers in domains and servers in workgroups will not work or will be extremely slow.
User Password	The valid password of the user specified above.

WM Publishing Points	Name	The publishing point on the VOD-WM (default = VBP) server where content will be accessed and managed by the ETV Portal Server. *Note: this setting must correspond to an existing, valid publishing point on the server.*
	Source	Local path to the publishing point. Default = d:/wmpub/WMRoot. Do not change for first publishing point.
	FTP Directory	Path to user-created FTP directory. See Creating a VOD-WM FTP Server.
	Low Space Threshold	Default = 20 MB. If the available disk space on this publishing point is less than the specified value, the publishing point with the largest amount of free space will be used.
	Free Space	The free space (in GB) available on disk is automatically recalculated when you add a new publishing point or refresh the publishing point list.

Adding Publishing Points to a WM Server

In a typical scenario, first you configure the publishing point on the Windows Media server, *then* you configure the publishing point on the Portal Server with matching values. Additional publishing points are required to make content available when you add disk space to a Windows Media server. As shown on the previous window, a Windows Media Server supports multiple publishing points. *In this context, publishing points are used to discover your content via FTP.* Use the following steps, **in the order shown**, to create a new publishing point. Note that as explained below, you must create a virtual FTP directory in IIS for *each* publishing point on the WM Server.

▼ To add a publishing point:

1. Create an FTP server on the WM server. See Creating a VOD-WM FTP Server on page 33.
2. Create a publishing point on the WM Server.
   a. Go to **Start > Administrative Tools > Windows Media Services**.
   b. Right-click on the server_name and select **Add Publishing Point (Wizard)**.
   c. Add a meaningful publishing point name and click Next.
   d. Select **Files (digital media or playlists) in a directory** and click Next.
   e. Select **On-demand publishing point** and click Next.
   f. Specify the location of your content, for example d:\WMPub\WMRoot and click Next.
   g. Skip through the remaining steps and click **Finish** when done.
3. To create a virtual directory on the WM server for this publishing point:
   a. Go to **Start > Administrative Tools > Internet Information Services (IIS) Manager**.
   b. Navigate to the Default FTP Website. Right-click and select **New > Virtual Directory**.
   c. For **Alias**, use the Publishing Point name from Step 3 above and click Next.
   d. Enter the path to the content directory for this FTP site and click Next.
   e. Allow **Read** and **Write** permissions and click Next.
   f. Click **Finish** when done.
4. In the Portal Server, configure the publishing point **Name**, **Source**, and **FTP Directory** to match the values you used for the publishing point on the Windows Media server.

© 2007 VBrick Systems, Inc.

Note

- The publishing point name within a server must be unique. You cannot add a publishing point that already exists in MCS database.
- The publishing point FTP directory within a server must be unique.
- If free space information is available at the time a publishing point is added, it must be greater than the entered Low Space Threshold.
- Publishing points located within another publishing point are not supported although publishing points on the same drive are supported. For example, two publishing points with **Source** `c:\pub1` and `c:\pub2` are supported but two publishing points with **Source** `c:\pub1` and `c:\pub1\pub2` are not supported.

Adding FTP Servers

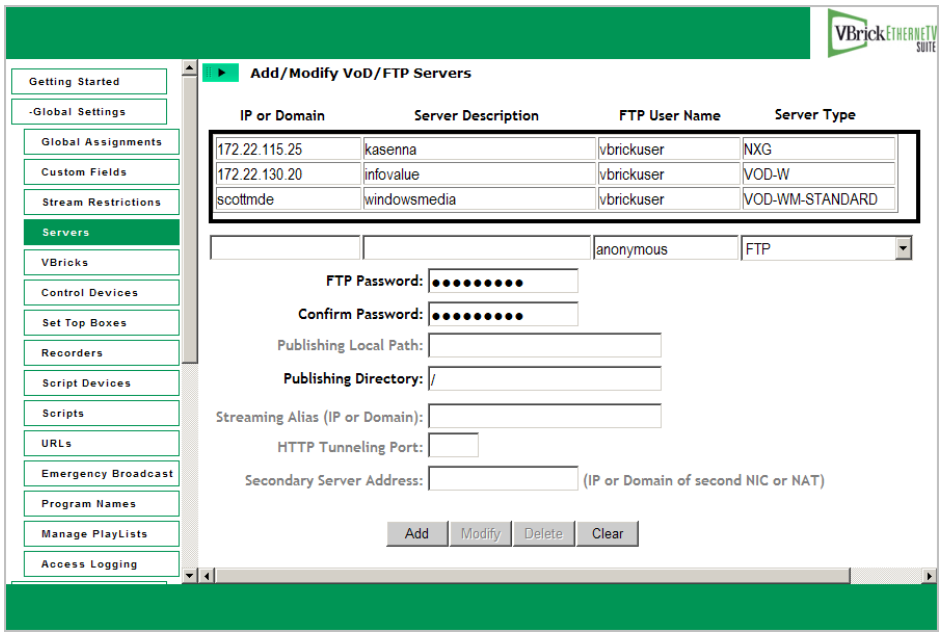


Figure 6. Add FTP Server

Creating a VOD-WM FTP Server

If you are using a VOD-WM-Enterprise or VOD-WM-Standard (Microsoft Windows Media) server, you must install and configure a standard FTP server on the VOD-WM server as explained below. (For more about Microsoft Windows Media servers see ETV Video-on-Demand Servers on page 6.)

▼ To create a Microsoft Windows Media FTP server:

On the Microsoft Windows Media Server:

1. Install the FTP server.
2. Set the default FTP directory to the Microsoft Windows Media Server's default Publishing Point directory.
3. Create and configure an FTP user account with full permissions (read/write, rename/delete etc.) on the directory specified above. If using the VBrick default, this account's user name is `vbrickuser` and the password is `vbrickuser`. Hint: use the settings of the `anonymous` account as an example.

4. Verify that the directory specified in Step 2 above is set to allow the FTP user account full permissions.

On the Portal Server:

5. When the Microsoft Windows Media Server is created or modified, specify the user name and password created in Step 3 above in the **FTP User Name** and **FTP Password** fields on the Add/Modify VOD/FTP Servers page

Creating a VOD-D FTP Server

If you are using a VOD-D (Darwin) server, you must install and configure a standard FTP server on the VOD-D server as explained below. (For more about Darwin servers see ETV Video-on-Demand Servers on page 6.)

▼ To create a Darwin FTP server:

On the Darwin Server:

1. Install a standard FTP server on port 21.
2. Set the default FTP directory to the Darwin Server's Media Folder directory (also called the Publishing Point) or create a virtual directory of the FTP root pointing to the Darwin server's Media Folder.
3. Create and configure an FTP user account with full permissions (read/write, rename/delete etc.) on the directory created above. If using the VBrick default, this account's user name is `vbrickuser` and the password is `vbrickuser`. Hint: use the settings of the `anonymous` account as an example.
4. Verify that the directory created in Step 2 above is set to allow the FTP user account full permissions.

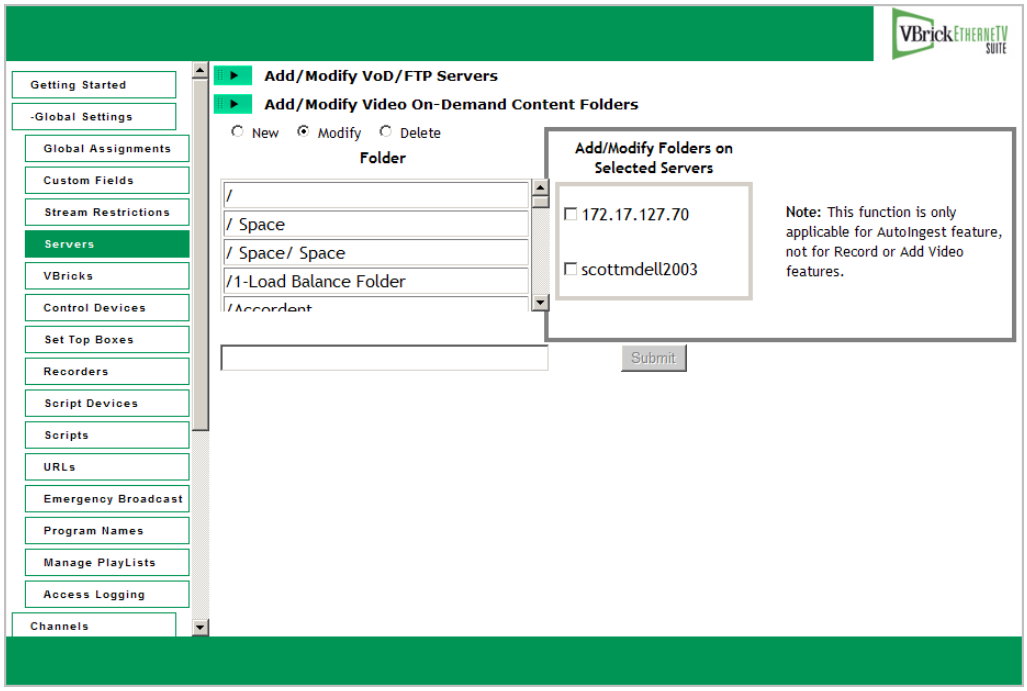
On the Portal Server:

5. When the Darwin Server is created or modified, specify the user name and password created in Step 3 above in the **FTP User Name** and **FTP Password** fields on the **Add/Modify VOD/FTP Servers** page.

Add/Modify Video On Demand Content Folders

Add/Modify Video On Demand Content Folders can be used to organize content on a specific Video-on-Demand server. The Portal Server periodically polls certain folders for presence of content and if found ingests the content onto multiple VOD servers. Any files FTPed into a particular folder in the Autoingest folder will automatically be ingested into the corresponding folder on the VOD server(s). You must add these folders using the window shown below. (See Auto Content Ingestion on page 119 for more about autoingestion.) Existing folder structures on a VOD server will be mirrored in the Portal Server. However you will still need to associate those folders with other server(s) if the file is to be autoingested onto multiple servers.

© 2007 VBrick Systems, Inc.



This function is useful for VBrick VBStar appliances to easily transfer content from their hard drives to the VOD server. (It can also be helpful for users who acquire content outside of the ETV Portal Server, for example from StreamPlayer Plus.) When a folder is created, you must check a box in **Add/Modify Folders on Selected Servers** to associate the folder with a server for autoingestion. ETV Portal Server checks these folders every 5 minutes and ingests new content if present. This feature only applies to Autoingest; it does not apply to **Record** or **Add Video**.

Note that empty folders are not displayed on the Portal Server client interface. These folders are only displayed when they have content. As the folder structure is created in this section, autoingest folders will be created in the FTP root path. For example, if the FTP root path is `d:\inetpub\ftproot`, then folders that are created in the **Add/Modify On-Demand** content folders will also be created in the `d\inetpub\ftproot\mcs\autoingest` folder.

Autoingested content can go into any folder that has been associated with a server or servers using the **Add/Modify Folders on Selected Servers** check boxes shown above. If using a VBStar, be sure to associate a folder with a server for autoingest. This enables the folder that the VBStar will FTP files into. This function is not associated with a user or group permission and is controlled only by the Administrator. See Auto Content Ingestion on page 119 for a more detailed description of the Autoingestion functionality.

Note Use the **Delete** button to remove non-empty folders only. Use the **Modify** button to change AutoIngest settings in the **Add/Modify Folders on Selected Servers** pane.

Creating Subfolders

Use the following steps to create a subfolder in an existing folder.

▼ To create a subfolder:

1. Highlight any existing folder name, for example `/Bill` as shown in the previous window, and click **New**.

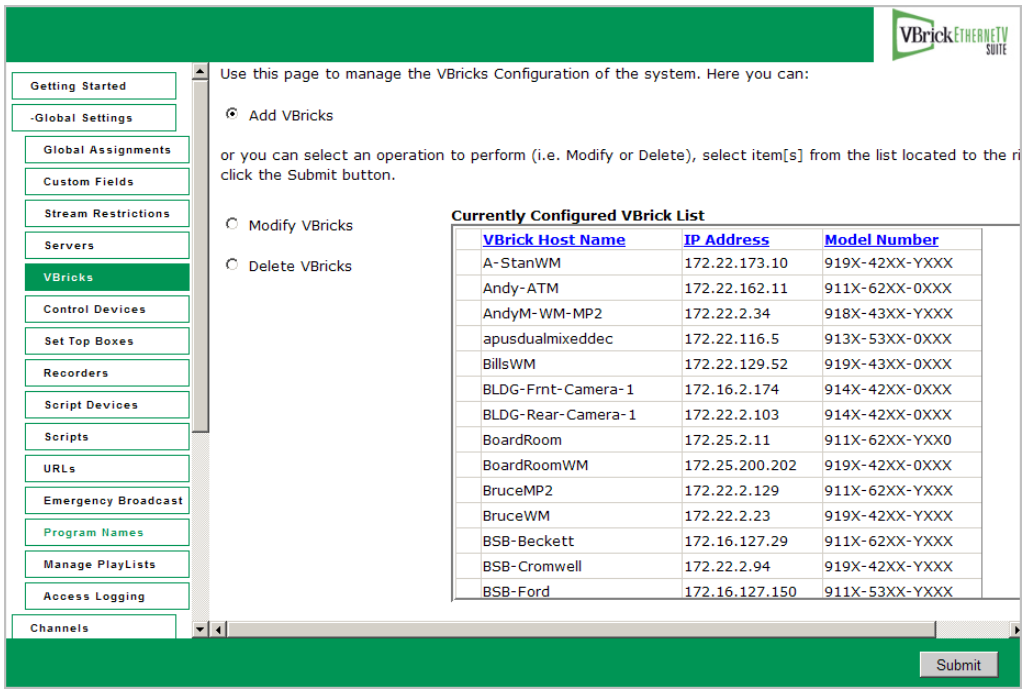
2. Type the new subfolder name in the text field, preceded by a forward slash, for example /Bill/**temp**, and click **Submit** when done.

VBricks

All VBricks must be configured in ETV Portal Server before they can be managed and used for scheduled events. (VBrick configuration is only required if you are using the **Scheduling** feature. Once configured, all VBricks in the system are shown on the following window. In the ETV Portal Server, SAP (Session Announcement Protocol) announcements are sent to the Portal Server by network-connected VBrick devices (encoders and/or decoders). The **Select VBrick** panel in the next screen shows VBrick appliances (encoders and decoders) that have announced their presence on the network but have not been configured for use in ETV Portal Server. (Note that if you delete a VBrick from the **Currently Configured VBrick List**, it will not be shown as available until you logout and log back in to the Admin Console.)

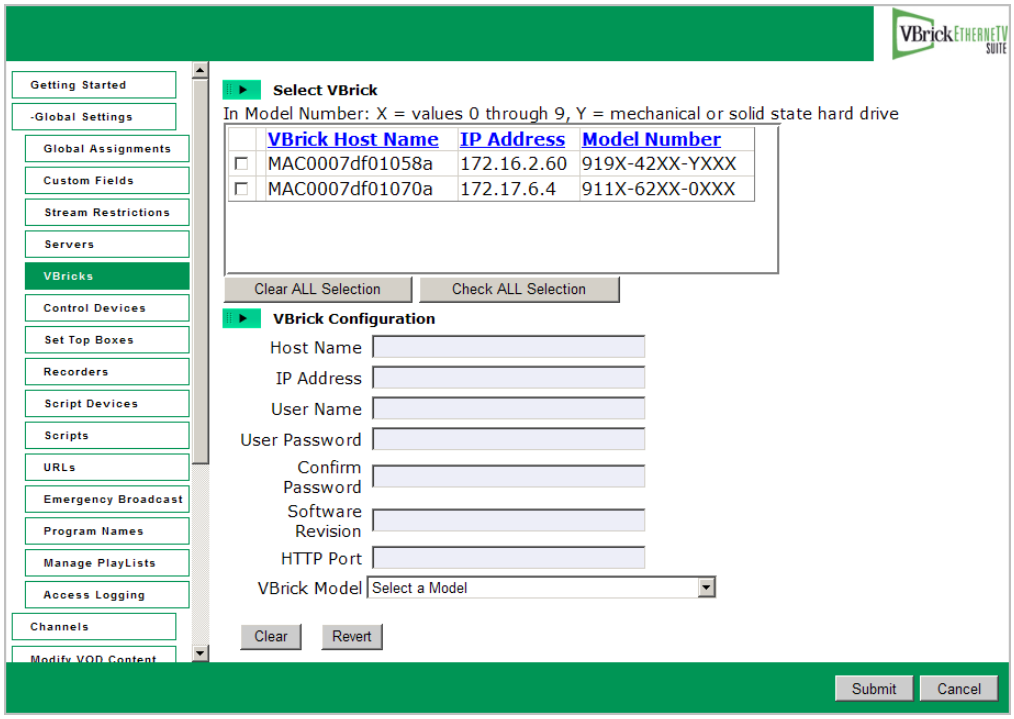
▼ To add a VBrick configuration:

1. Go to **Global Settings > VBricks**.



2. Select **Add VBricks** and click **Submit**.

© 2007 VBrick Systems, Inc.



3. In **Select VBrick**, select one or more existing VBricks for which a SAP has been received. If you select one VBrick, this populates the **VBrick Configuration** panel. (If you select multiple VBricks, it does not populate the panel; if you need to configure the VBricks, you must add them one at a time.)
4. Complete or modify the fields in **VBrick Configuration** as necessary. Note that you must enter a User Name and Password and confirm that Password or the configuration will fail.
5. Click **Submit** when done. This adds the new configuration to the list of configured VBricks shown on the previous page.

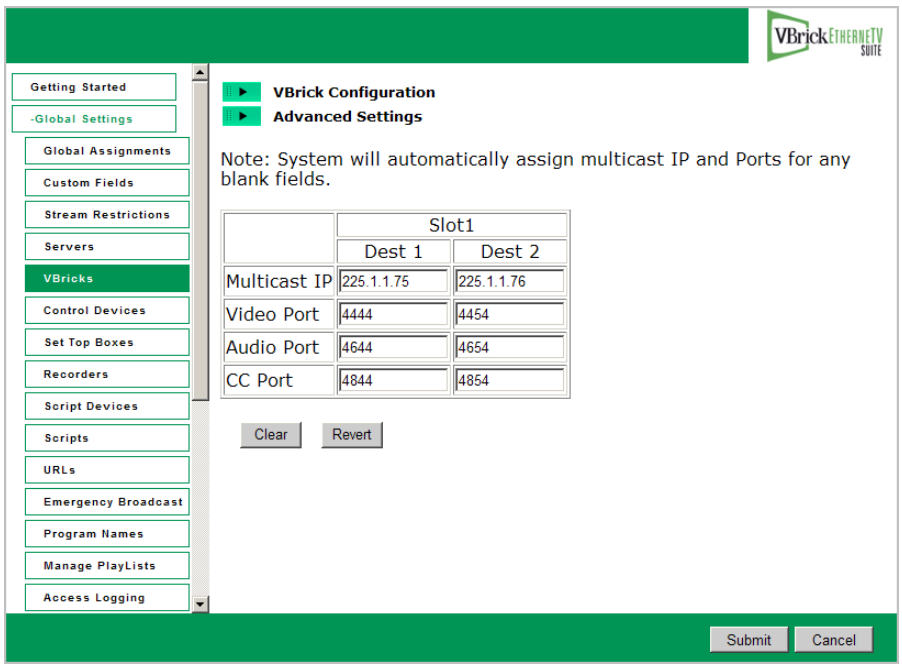
Note The only time you will manually complete the VBrick Configuration fields is when you are defining the configuration for a VBrick that will be added to the network at a later time. In this case, you will need to know the following configuration data in advance.

Host Name	Required. Host name of VBrick.
IP Address	Required. IP address of VBrick.
User Name	Defaults to system-defined value if blank.
User Password	Defaults to system-defined value if blank.
Confirm Password	Defaults to system-defined value if blank. Must match User Password if entered above.
Software Revision	Optional. To get the Software Revision in IWS, go to **Status > System Information >** Release Revision.
HTTP Port	Optional. To get the HTTP Port in IWS, go to **Configuration > System > Security > IWS Server Port**.

VBrick Model	Select from dropdown. Advanced settings are enabled if you select an encoder or a VBStar.

Advanced Settings

Advanced settings are enabled if you select a VBrick encoder or a VBStar. *Note that the Portal Server will attempt to retrieve and autofill the Multicast IP addresses and Port numbers.* You can modify these fields as necessary.



Note The following values are stored in the Portal Server database only. Depending on how a scheduled event is configured, they may be saved and written back to the VBrick device after the scheduled event runs.

Multicast IP	Destination multicast IP address.
Video Port	Destination video port.
Audio Port	MPEG-4 devices only. Destination audio port.
CC Port	MPEG-4 devices only. Closed captioning port.

Control Devices

Control devices let you configure a video source device so that it can be controlled by end users from the Portal Server user interface. (An example of a video source device is a DVD or VCR directly connected to a VBrick encoder.) Once configured, a special icon on the **Live Broadcasts** page indicates you can control the stream using a "virtual" remote control panel as shown in Figure 7 below. VBrick currently supports DVDs and VCRs from several different manufacturers as well as the VBrick VBIR remote controller that can be customized for use with a wide variety of source devices. See Adding User-Defined VBIRs below for more about VBIRs.

© 2007 VBrick Systems, Inc.

Note In some cases you may be able to control a source device using the front panel or the handheld remote that came with the unit, but this is not always possible. For example, if the remote gets lost or the source DVD and/or VCRs are rack-mounted in an inaccessible metal enclosure, you *must* use the Portal Server interface or a VBIR.

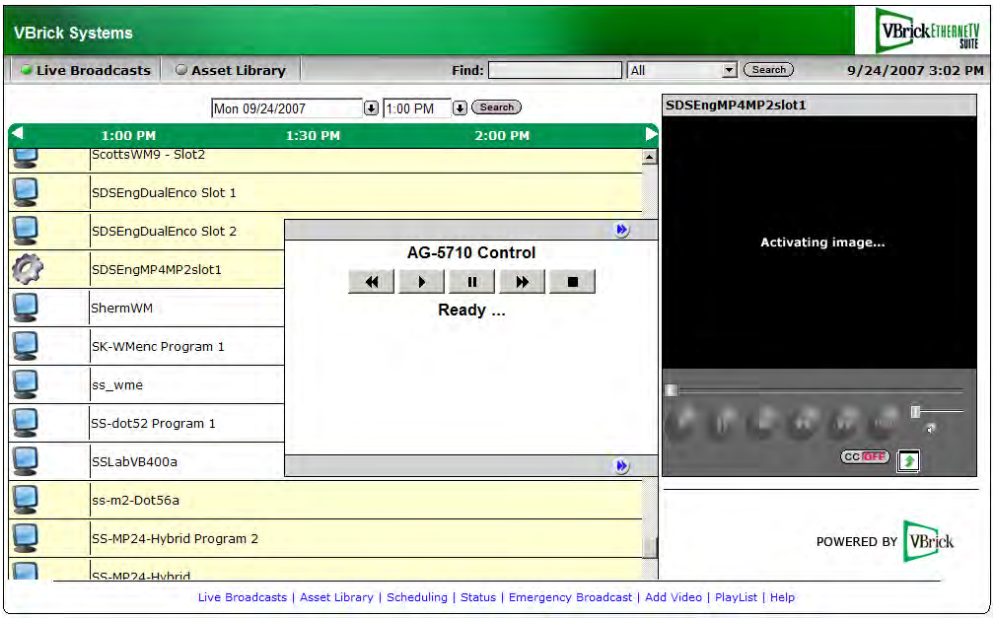


Figure 7. "Virtual" Remote Control Panel on Live Broadcasts Page

As shown in Figure 8 below, the remote control panel will have a different graphical user interface depending on whether the source device is directly attached (via a serial port connection) or uses a VBIR. The control panel interface for direct-connect devices varies according to the specific device you select; the control panel interface for VBIR-connected devices is the same for all VBIR devices.

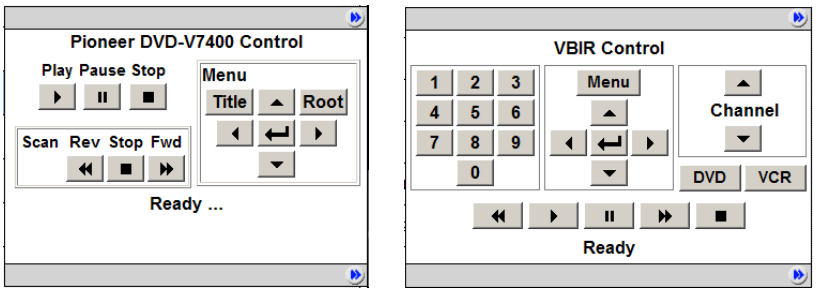


Figure 8. Control Panel for Direct-Connect Devices (left) and VBIRs (right)

Note The Amino set top box does not recognize "control devices." Any video source devices configured as **Control Devices** in the Portal Server will not display a "virtual" remote control panel on the Amino set top box.

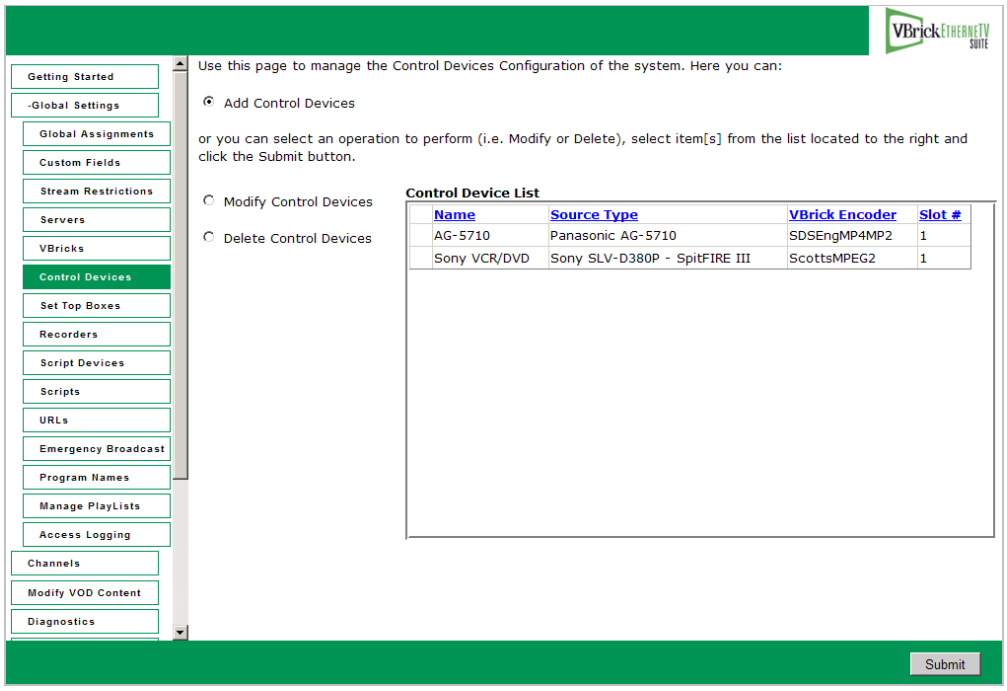
Adding Control Devices

Use the following windows to define or modify control devices. As noted, these devices will be displayed on the **Live Broadcasts** page with a special icon for any users with access to that

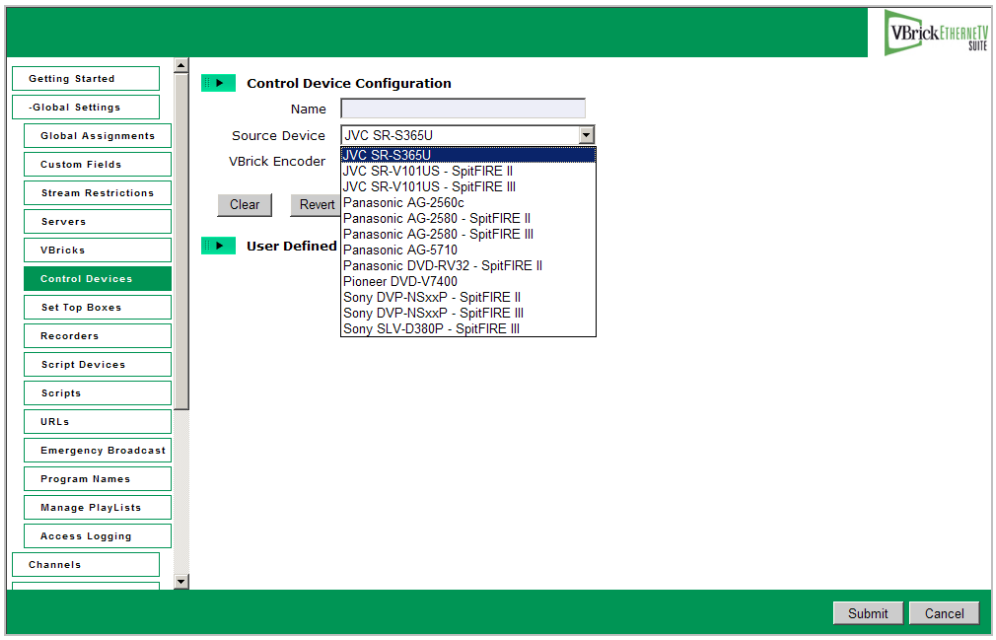
encoder. *If the device is used as a source encoder for a scheduled broadcast, however, only the user who actually created the schedule will have access during the scheduled period.* This prevents other users from potentially interrupting the broadcast. If the Portal Server does not have a Scheduling license, all control devices are available at any time to any user with VBrick access and other permissions. See "Using the Scheduler" in the *Portal Server User Guide* for an explanation of how to schedule events for control devices.

▼ To define a control device:

1. Go to **Global Settings > Control Devices** and select **Add Control Devices**.



2. Complete the fields on the next screen as explained below and click **Submit**.



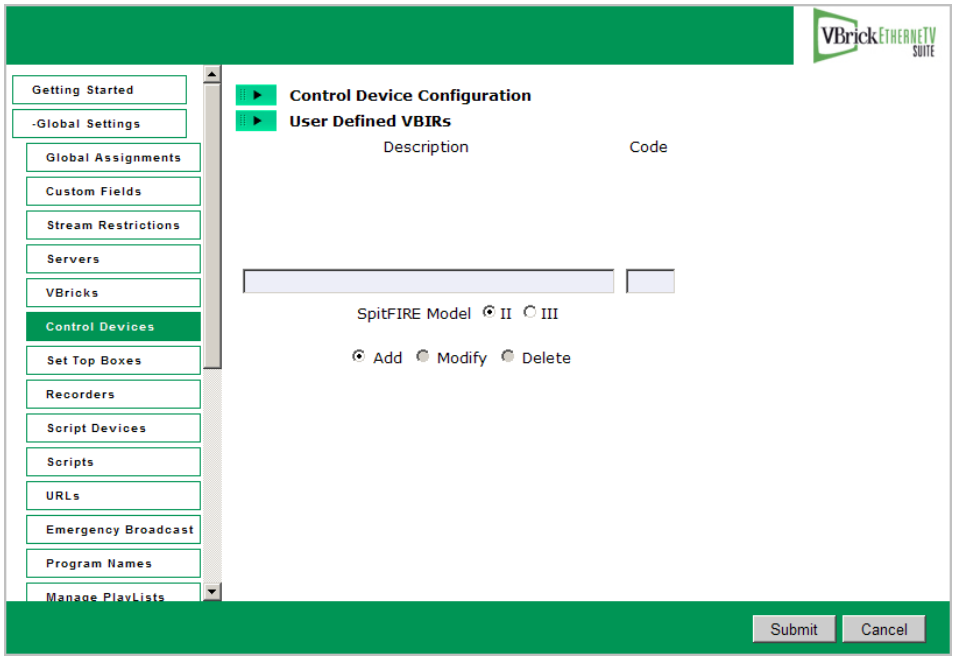
© 2007 VBrick Systems, Inc.

Name	Enter a unique, descriptive name that will be displayed on the virtual remote. For example in Figure 7, "Sony DVD" is the configured name shown on the controller. No embedded spaces or special characters are allowed.
Source Device	Select a source DVD or VCR from the dropdown list. The list shows serial port direct-connect devices and VBIR (SpitFire) devices that are tested and supported by VBrick. It also shows any custom VBIR devices you have added (note that you cannot add serial port direct-connect devices). You add custom devices by creating a User Defined VBIR as explained below. If the source device you wish to control does not have a serial port, you *must* use a VBIR for remote control.
VBrick Encoder	Select the specific encoder to which the selected Source Device above is connected from the dynamically populated list of encoders on your network.
User Defined VBIRs	Select the SpitFire version you have (SpitFire II or III) and enter a Description and a three-digit Code (see Adding User-Defined VBIRs below).

Adding User-Defined VBIRs

The VBrick VBIR is an external hardware device that uses the passthough port on a VBrick to send control commands *via an infrared link* to third-party devices like VCRs, DVDs, etc. (see Figure 9 for a visual schematic). You must use a VBIR if the target third-party device does not have a serial port that can directly connect to a VBrick encoder. The VBIR can be programmed with codes representing IR command sets that are compatible with devices from many manufacturers. Use the following window to create a custom **User Defined VBIR**. Enter a device description (20 characters or less), a three-digit code, and select the SpitFire model. When done, the new device is added to the **User Defined VBIRs** list as well as to the **Source Device** dropdown list. For a current list of VCR/ DVD device codes for SpitFire II models, go to http://innotech.com/spitfire-ii-device-codes.pdf For SpitFire III models, go to http://innotechsystems.com/Spitfire/SpitFire III.pdf Be aware that the device codes at this link are not tested or supported by VBrick. If you can't find the code you need, or have trouble controlling a non-supported device, check the product documentation or contact the manufacturer.

Note The VBIR (**SpitFire III model only**) can also "learn" (i.e. be programmed to use) IR commands much like a universal remote controller. Learned commands are stored in VBIR memory areas called slots and are accessed by reserved three-digit codes. The six slots are available are: AUX (994), TV (995), VCR (996), DVD (997), AUD (998), and CBL/SAT (999). For a detailed explanation of how a VBIR "learns" commands, see the Application Note Learning IR Commands on the VBIR on the VBrick Product Documentation website.



Connecting Control Devices

To set up a device that can be remotely controlled from the Portal Server, you connect the serial interface on the source device (the DVD or VCR) to the passthrough port (COM1 or COM2 for Slots 1 and 2 respectively) on the VBrick encoder using an appropriate cable (see Table 10) from those shipped with the encoder. For more about Serial Port Passthrough, see the online help for the encoder. You can also control devices using VBrick's VBIR remote controller. To use the VBIR remote controller, you connect the VBIR SpitFire device to COM1 or COM2 on the VBrick encoder. The VBIR subsequently communicates with the DVD or VCR via infrared commands (see Figure 9) at the configured baud rate.

If necessary, connect one end of the XIR emitter cable to the SpitFire and the other to the DVD or VCR making sure the adhesive lead is securely attached to the device. The emitter is used when there is no direct line-of-sight to a control device (for example when the VCR is in a cabinet) and you can't use the remote control. On the back of the VBIR, be sure the SpitFire is in RS-232 mode.

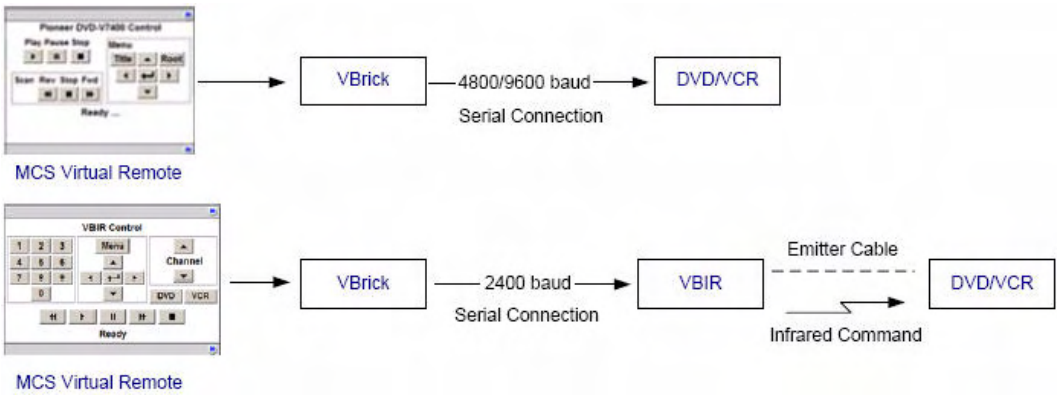


Figure 9. Connecting Control Devices

© 2007 VBrick Systems, Inc.

Table 10. Device Connectors

Device	Connector
VCR	DB-9 †
DVD	DB-15 †
MPEG-1 Encoder	DB-9
MPEG-2/4/WM Encoders	RJ-45

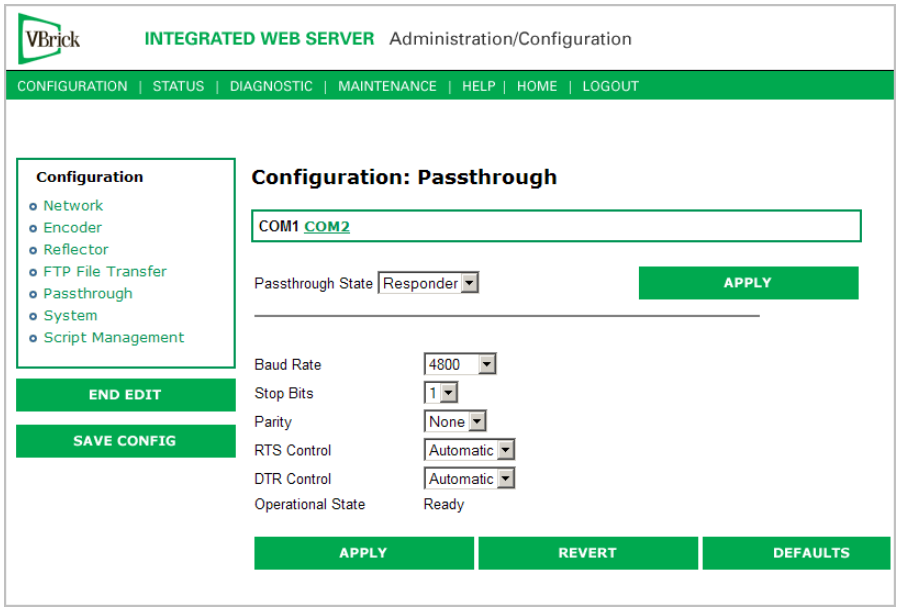
† Typical device connector.

Configuring Control Devices

You also need to configure the baud rate and passthrough state of the VBrick associated with a control device. In IWS, go to the **Configuration: Passthrough** page and set these values as follows:

Table 11. Baud Rate and Passthrough State

Device	Baud Rate	Passthrough State
DVD	4800	Responder
VCR	9600	Responder
VBIR	2400	N/A



Control Device VBIRs

EtherneTV Portal Server Control Devices use SpitFIRE model VBIRs to manipulate DVDs, VCRs or other devices controlled by IR commands. The VBIR contains an internal library of several hundred IR command sets stored in flash memory. The internal library is accessed by a three digit code. The VBIR internal library supports a wide range of devices from many, but not all, device manufacturers. If the IR command set for a particular device is not stored

in the internal library there are two ways that the VBIR can be enhanced to control the device.

Learning IR Commands

The VBIR can be set to learn and store IR commands like a universal remote. Once learned IR commands are stored on a VBIR they can be written as an external library file on a PC. The IR commands in an external library file can be learned by other VBIRs through the process of cloning. For more information, see the application note Learning IR Commands on the VBIR on the www.vbrick.com/documentation page.

Downloading External Libraries

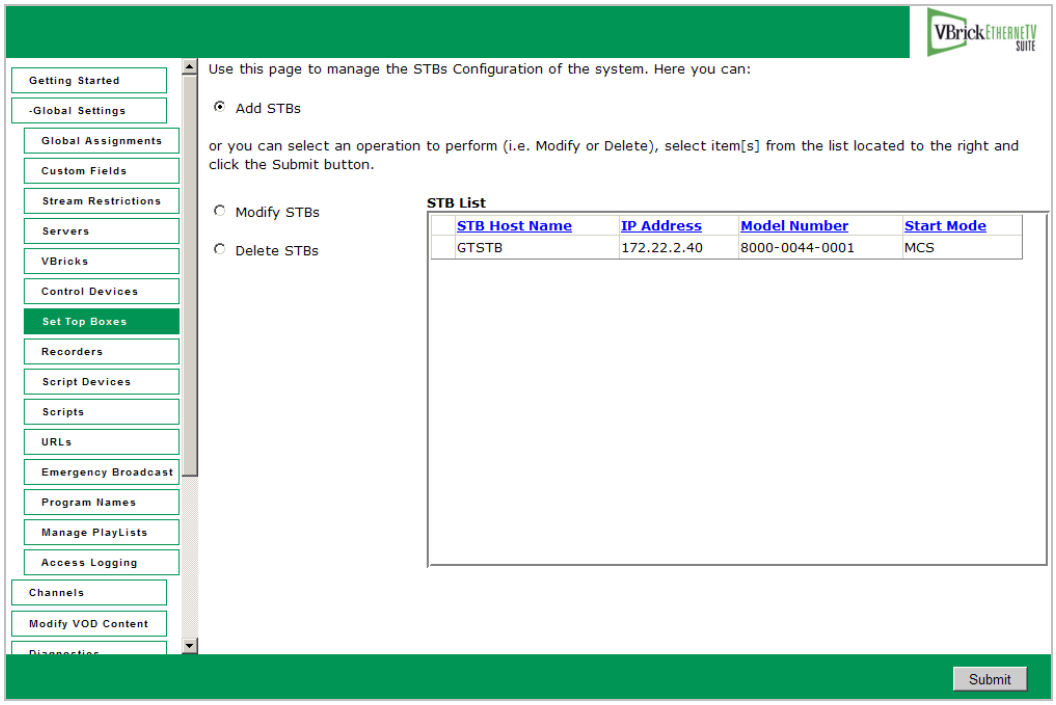
The VBIR can be upgraded by downloading an external library file. External library files contain IR command sets for a specific device or devices. External library files are supplied by a third party or created using the SpitFIRE VBIR learning mode. For more information, see the application note Downloading External Libraries to the VBIR on the www.vbrick.com/documentation page.

Set Top Boxes

STBs (Set Top Boxes) must be configured in ETV Portal Server before they can be managed and used for scheduled events. (STB version must also be 3.7.1 or higher.) Once configured, all STBs in the system are shown on the following window. The **Select STB** panel in the next screen shows STBs that have announced their presence on the network but have not been configured for use in the Portal Server.

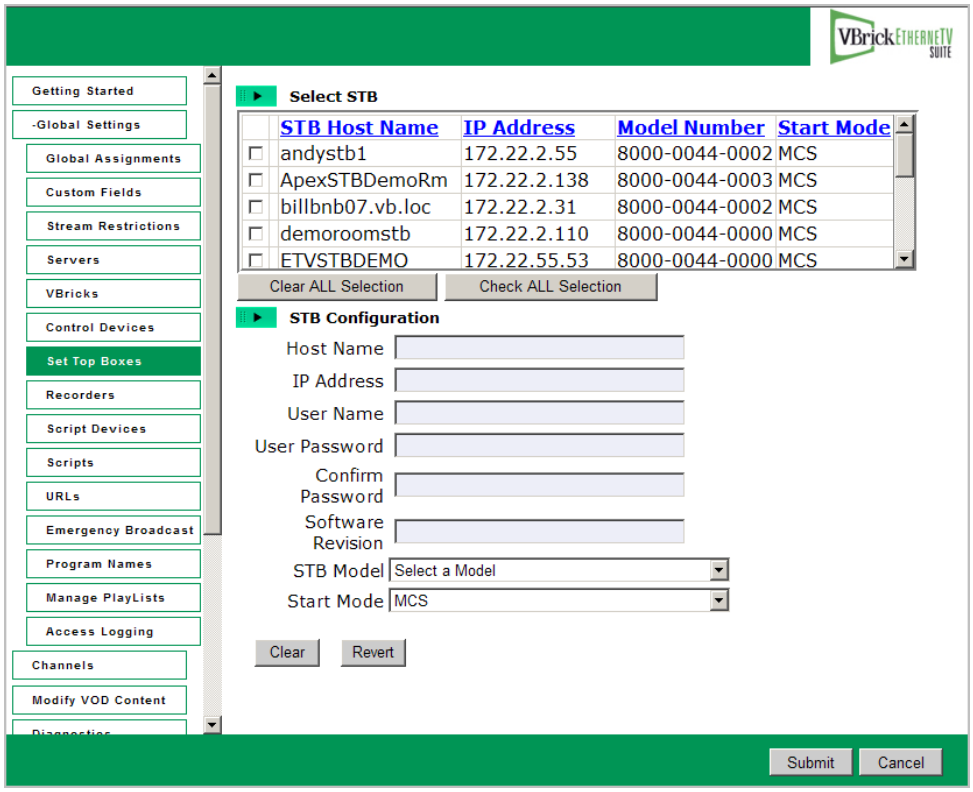
▼ To add an STB configuration:

1. Go to **Global Settings > Set Top Boxes**.



2. Select **Add STBs** and click **Submit**.

© 2007 VBrick Systems, Inc.



3. In **Select STB**, select one or more existing STB for which a SAP has been received. This populates the **STB Configuration** panel. (If you select multiple STBs, it does not populate the panel; if you need to configure the STBs, you must add them one at a time.)
4. Complete or modify the fields in **STB Configuration** as necessary and click **Submit**. This adds the new configuration to the list of configured STBs shown on the previous page.

Note The only time you will manually complete the STB Configuration fields is when you are defining the configuration for an STB that will be added to the network at a later time. In this case, you will need to know the configuration data in advance.

Host Name	Required. Host name of STB.
IP Address	Required. IP address of STB.
User Name	Defaults to system-defined value if blank.
User Password	Defaults to system-defined value if blank.
Confirm Password	Defaults to system-defined value if blank. Must match User Password if entered above.
Software Revision	Optional.
STB Model	Select from the dropdown.
Start Mode	Select from the dropdown: ETV Portal Server, Local, or Local-Fullscreen

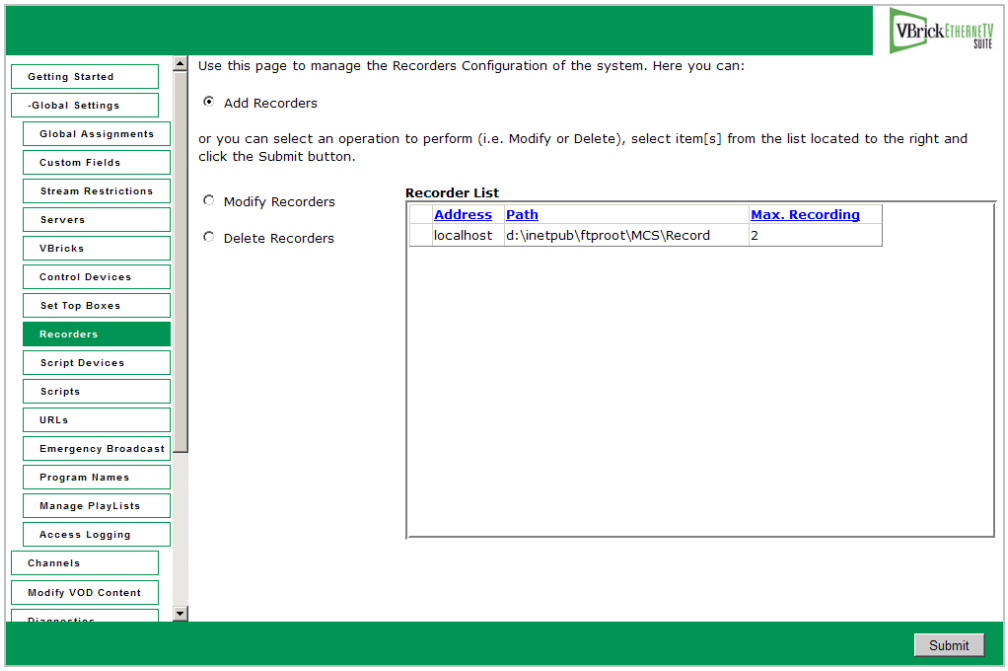
Recorders

A Recorder server enables recording by Portal Server users. If a recorder server is not created here, any attempt to record a live stream or a stored video will fail. Once enabled, users must also be assigned the appropriate permissions (see Allow Content Recording on page 96). (Note: Do not confuse a Recorder server with a Network Video Recorder which is a a separate product. See the *ETV Network Video Recorder Release Notes* for more information.)

Note By installation default, all recordings are stored on the D: drive. If you install ETV Portal Server on a system without a D: drive, you must subsequently go to **Global Settings > Recorders** and change the record path as necessary. Also, the **Max Recording** field shows the default number of concurrent recording sessions allowed. *If you need more than 2 concurrent recording sessions, you must purchase a Network Video Recorder.*

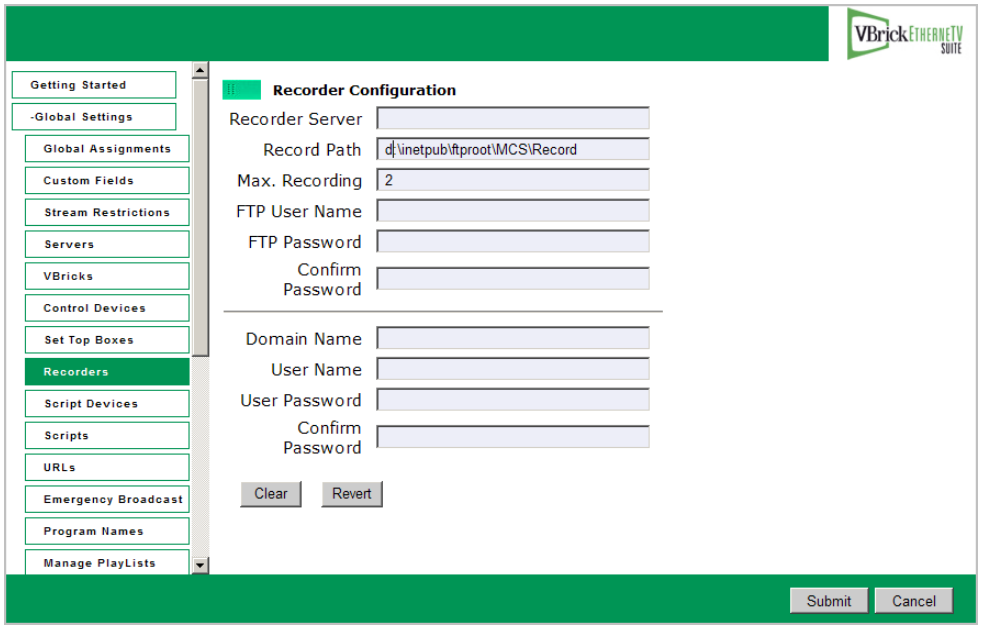
▼ To add a Recorder configuration:

1. Go to **Global Settings > Recorders**.



2. Select **Add Recorders** and click **Submit**.

© 2007 VBrick Systems, Inc.



3. Complete the fields in **Recorder Configuration** window and click **Submit**. This adds the newly configured recorder to the previous window. If necessary see Synchronizing the Portal Server and the NVR below.

Recorder Server	IP address or host name of recorder server. Defaults to localhost if recorder server is on the same machine as ETV Portal Server.
Record Path	Path and folder where all recording are stored. By default, recordings are stored on the D: drive. If you install ETV Portal Server on a system without a D: drive, you must change the path. Also, in order to record multiple streams, the Record Path must be under FTP root. For example, if root is `C:\Inetpub\ftproot` the Record Path must be `C:\Inetpub\ftproot\<your_folder>`
Max. Recording	The default number of concurrent recording sessions allowed is 2. If you exceed 2, you must purchase a Network Video Recorder. Without an NVR, any attempt to record more than 2 concurrent sessions will fail.
FTP User Name	FTP user name in operating system of Recorder server.
FTP Password	FTP password in operating system of Recorder server.
Confirm Password	FTP password in operating system of Recorder server.
Domain Name	*This field is required only if the Recorder server is not on the local network.* Enter the domain name if the Record Path above points to a server in a different domain,
User Name	The user name who has access to the specified path.
User Password	The corresponding password for this user name.

Synchronizing the Portal Server and the NVR

The internal clocks on the Portal Server and the NVR must be synchronized for recording functionality to work properly. You can use the `Net time` command as explained below or you

can use an external time server. In order to run the `Net time` command on *either* server, the server must be on the domain, and the user logged onto the server must have admin privileges *and* be part of the domain. To synchronize the Portal Server and the NVR use the following command:

- Windows 2003 Server – Open a command prompt on the *Portal Server* and type:
  `Net time \\{NVR IP Address} /SET`

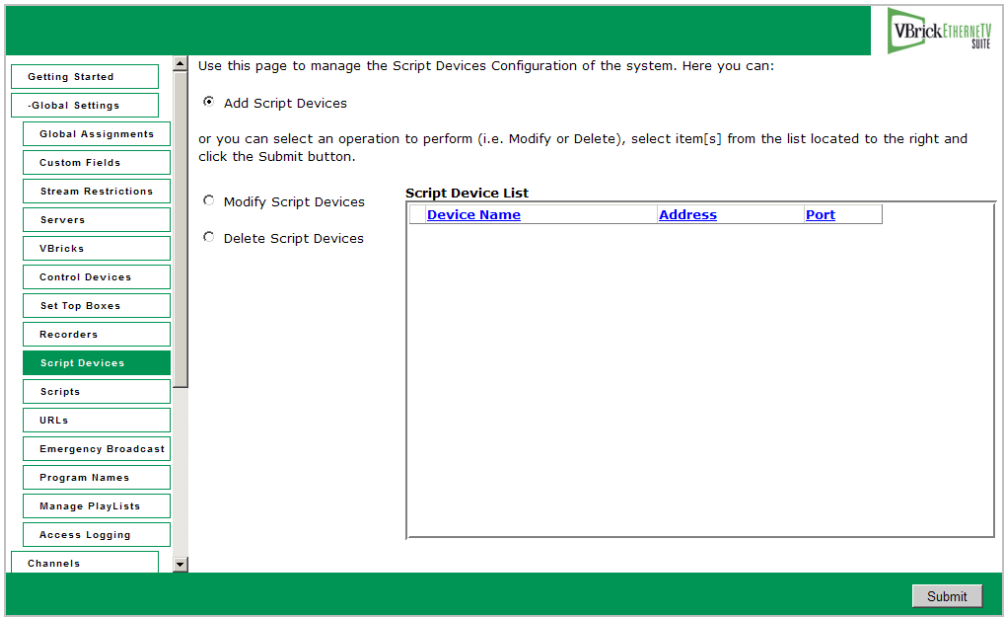
Script Devices

Script devices work with scripts and can be used to control VBricks, or other devices attached to a VBrick via the serial port. In order to use a script, the device (a VBrick, STB, camera, VCR, etc.) must be defined in the Portal Server database as a script device. Once defined, they can be subsequently controlled by a script (see Scripts on page 49) launched from the Portal Server Scheduler. A script device must be physically connected to the network and must be available at the runtime of a scheduled event. For example, PTZ cameras respond to pan, tilt, and zoom commands. Once defined as a script device, pan, zoom, and tilt commands can be scripted and executed from ETV Portal Server to control the movement of the camera at a specific date, time, and recurrence.

Note You can also write a script (launched from the Portal Server) that uses TCP/IP to communicate with any compatible device on the network. Contact VBrick Support Services for more information.

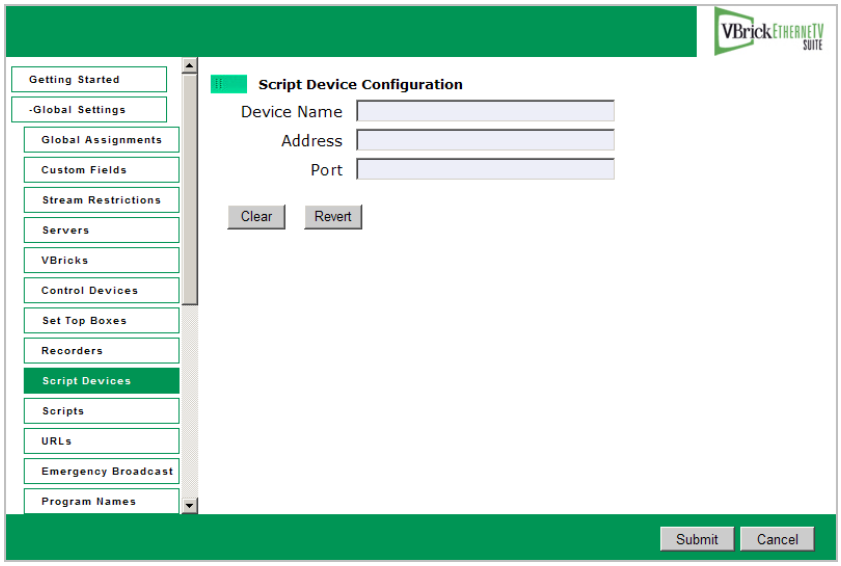
▼ To add a Script Device configuration:

1. Go to **Global Settings > Script Devices**.



2. Select **Add Script Devices** and click **Submit**.

© 2007 VBrick Systems, Inc.



3. In **Script Device Configuration**, complete the following fields and click **Submit**. This adds the newly configured script device to the list of devices shown in the previous window. To modify a Script Device, first delete the device and then repeat these steps.

Device Name	Any user-defined name.
Address	Hard-coded device IP address. This is usually the address of the VBrick or the address of the VBrick to which a device is connected but it can be the address of any device.
Port	TCP/IP port number range = 1040–65534. If using serial port passthrough, use the VBrick's passthrough port number: 4439 for COM1, 4414 for COM2

Scripts

Scripts work with previously defined script devices such as VBricks, STBs, or other devices attached to a VBrick. Scripts can be used to control any type of VBrick or to control other devices like cameras and VCRs that are attached to a VBrick. To script VBrick commands, you select the VBrick and build a script by choosing parameters from a dropdown list—the parameters vary depending on the type of VBrick you select (MPEG1, MPEG2, etc.). You can script commands to change any of the parameters (in the MIB database) that are available through IWS.

For non-VBrick (**Other**) devices, you write a script from scratch using the native language for that device. This scripting functionality is designed for advanced users and you must know the instruction set for the device in order to script commands that will control that device. You can use a text-based script or a binary script to control devices connected to the serial passthrough port (COM1 or COM2) on a VBrick encoder.

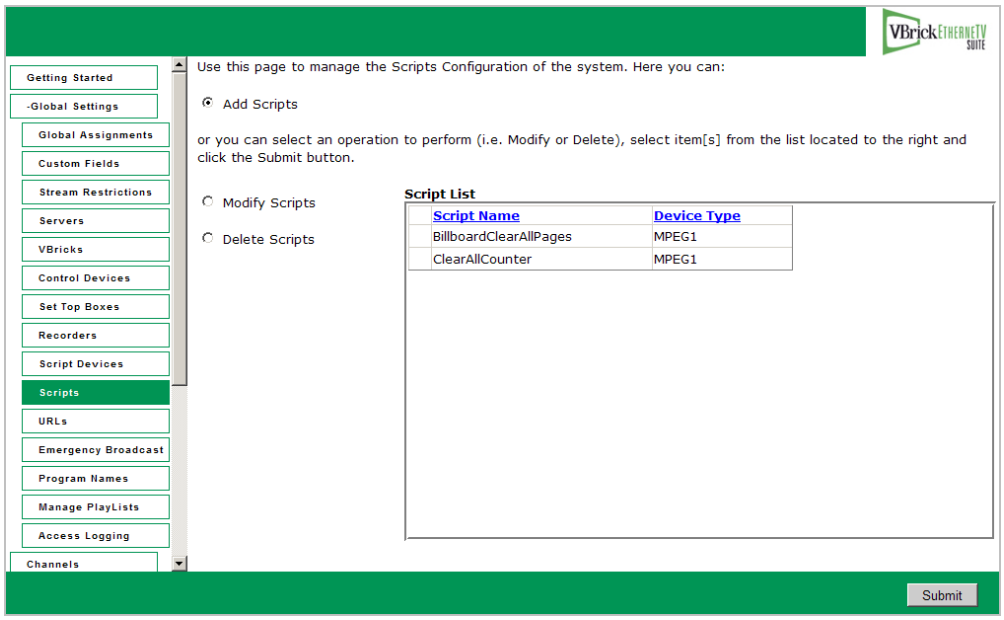
You can control devices that require binary input by pasting binary input into the **Script Content** text box. Binary scripts let you provide a sequence of commands for devices that require binary input. This type of script will pass binary input through the serial passthrough port on a VBrick to the specified device. You will typically connect your device to the serial passthrough port using the port number previously defined for the device (4439 for COM1, 4414 for COM2).

Note If you are scheduling an event, any device for which you write a script must be available to the network at runtime. If the device is not available the script will fail.

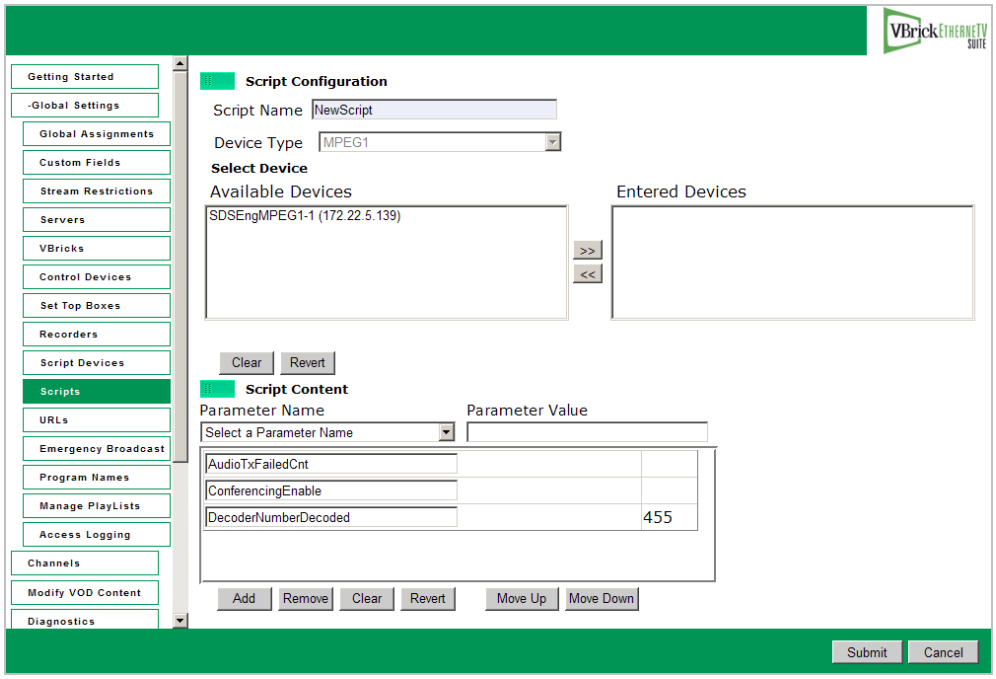
Creating a Script

▼ To create a script that can be executed from the Portal Server:

1. Go to **Global Settings > Scripts**.



2. Select **Add Scripts** and click **Submit**.



© 2007 VBrick Systems, Inc.

3. In **Script Configuration**, enter a **Script Name** and select a **Device Type** (MPEG1, MPEG2/MPEG4/WM, or Other) from the dropdown list—and wait a few seconds for ETV Portal Server to populate the panel with a list of devices.
4. In **Select Device**, highlight one or more devices and use the arrow buttons to populate the right panel.
5. Create the **Script Content**.
   a. For VBrick devices, select a **Parameter Name** from the dropdown list , enter a **Parameter Value**, and click **Add**. Repeat as many times as necessary and click **Submit** when done. Note that the order in which you add parameters is critical. This is the order in which the commands will be executed at runtime. (See Finding VBrick Parameters and Values for more information.
   b. For non-VBrick (**Other**) devices, write the script in a native language compatible with the device (or copy and paste binary input) and click **Submit** when done.

To run a previously created script, login to ETV Portal Server and click **Scheduled Programs**. Then create a schedule by selecting a date, time, and (optionally) a recurrence pattern. When done, click **Script** and select the script you want to run on the schedule you just defined.

Example

The following example shows binary input for a VBrick VBIR device. In a typical scenario you will need to set the **Passthrough State** and other parameters on the encoder before you can run the script. See "Serial Port Passthrough" in the *VB4000-5000-6000 Admin Guide* for more information. The following example programs a VBrick VBIR device to device code 351 and sends the Play command. This is just a brief example. If you need help or want more information about using binary scripts, please contact VBrick Support Services.

Begin instruction set, program for following device code. *This set of instructions is used in all scripts.*

```
<-script->
<-send binary 0xc1 0x0d->
<-receive 2->
<-send binary 0xc0 0x0d->
<-receive 2->
```

Program three-digit device code. Here code is 351.

```
<-send binary 0x83 0x0d->
<-receive 2->
<-send binary 0x85 0x0d->
<-receive 2->
<-send binary 0x81 0x0d->
<-receive 2->
```

End device code programming, set for command. *This set of instructions is used in all scripts.*

```
<-send binary 0xc0 0x0d->
<-receive 2->
<-send binary 0xd3 0x0d->
<-receive 2->
```

Command. Here Play.

```
<-send binary 0x91 0x0d->
```

```
<-receive 2->
```

Finding VBrick Parameters and Values

In order to create scripts, you need to determine the correct parameters and values to use. The following procedures explain how to locate parameters from the IWS page and how to find the value associated with that parameter using a standard MIB browser or text editor. These brief procedures simply outline the basic steps which are typically performed by a programmer or a system administrator. Contact VBrick Customer Service or see the *VBrick SDK User Guide* for more information.

▼ To locate a parameter name by viewing the source code:

1. Find the **Parameter Name** in the Integrated Web Server (IWS) page.
2. Then locate the parameter name by viewing the source code of the page.

▼ To find the parameter value:

1. Locate the parameter name as described above.
2. Find the **Parameter Value** by examining the MIB file with either a standard MIB browser or a text editor.

URLs

Add/Modify a URL for a Live Video Stream

Administrators can manually enter URLs to live video streams that will not automatically be displayed by the Portal Server. For example, the administrator may wish to have the Announcements (SAPs) disabled on the VBrick encoders for security purposes. Or the Administrator may want to enter the address of an off-network stream such as an MPEG-4 Stream from an Apple Darwin Server or a stream coming from a hosting provider. Additionally, this feature lets you enter the addresses of non-MPEG streams such as Windows Media and Real Networks. Note that the Access Control feature Allow Viewing by Content Type does not apply to manually added URLs. You can also filter and control which live streams are shown in the Portal Server by using a bit mask on the VBrick encoder. For more about this feature, refer to the Category parameter in the appropriate MPEG-2, MPEG-4, or WM encoder documentation. In IWS, go to **Configuration: Encoder > Announce (SAP)**.

Note For any non-MPEG video, the correct player (such as Windows Media Player or Real Player) must be present on the desktop for the client to be able to receive the stream. Set Top Boxes will not be able to receive non-MPEG streams because the Set Top Box only includes decoders for MPEG-1, MPEG-2, and MPEG-4.

The following examples show valid URL syntax for live video streams. All URLs are case sensitive. The syntax must be accurate and there is no internal validation of user input:

Valid for Types MPEG-1 and MPEG-2

```
vbricksys://ip=239.1.1.1&port=4444
```

Where `239.1.1.1` is the multicast IP address and `4444` is the multicast port.

Valid for Type MPEG-4

```
rtsp://172.1.1.1/vbrickvideo1
```


© 2007 VBrick Systems, Inc.

```
vbrtsp://172.1.1.1/vbrickvideo1
```

Where `172.1.1.1` is the source IP address and `vbrickvideo1` is the program name.

```
vbhttp://172.1.1.1/vbs2d1.sdp
```

Where `172.1.1.1` is the source IP address and `vbs2d1.sdp` is the SDP file name.

Valid for Type Other

ASX Files

```
http://172.1.1.1/file.asx
http://myHost/file.asx
http://www.myCompany.com/files/file.asx
```

MP3 and WMA Files

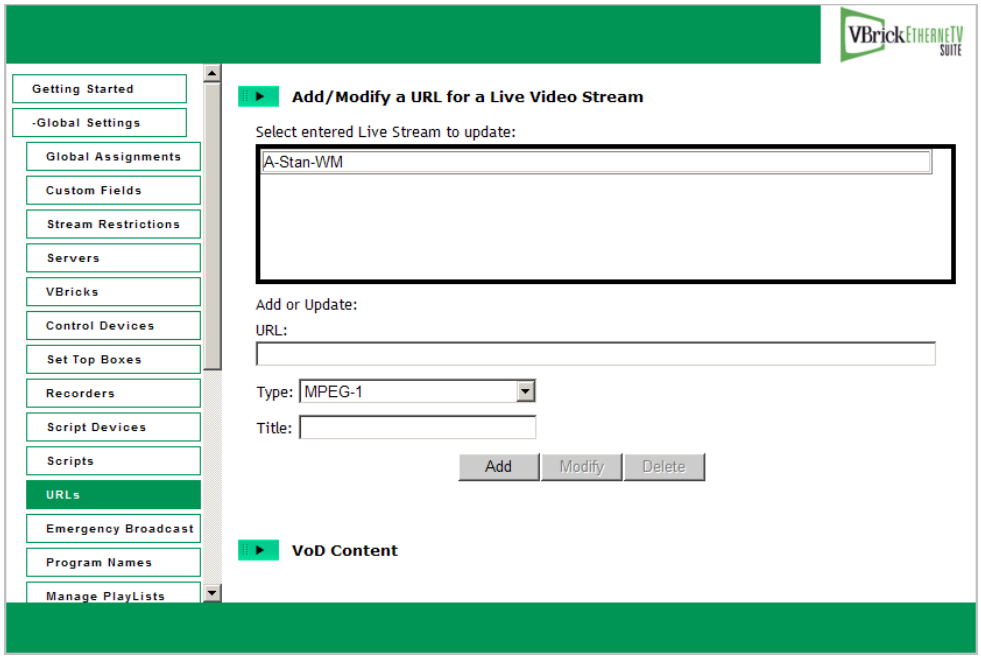
```
http://172.1.1.1/file.mp3
http://myHost/file.mp3
http://172.1.1.1/file.wma
http://myHost/file.wma
```

WMV Files

```
http://www.myCompany.com/files/file.wmv
mms://www.myCompany.com/files/file.wmv
```

▼ To add a URL for a live video stream:

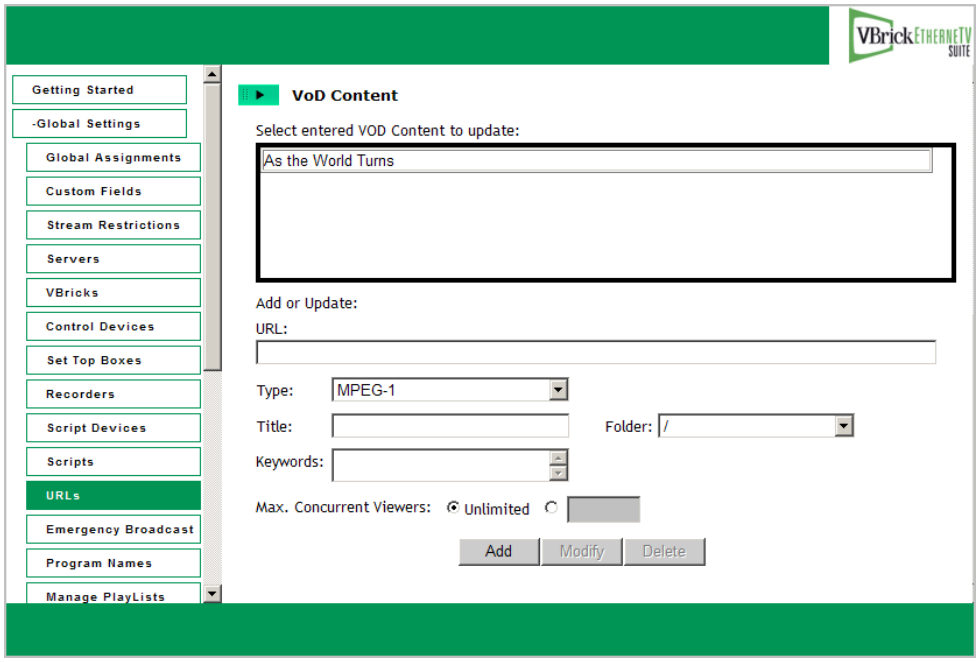
1. Enter the URL or IP address in the **URL** field.
2. Enter the **Type** and **Title** and click **Add** to add the URL to the list of streams shown.



URL	Enter a valid URL or IP address. See examples above.
Type	Choose MPEG-1, MPEG-2, MPEG-4, WM or Other. Select Other for most non-MPEG streams; select WM for .swf Flash streams.
Title	Title is what will display to clients in the ETV Portal Server viewing pages.

Add VOD Content

Administrators can manually enter URLs to VOD content that is not automatically displayed by the Portal Server. These URLs can be to content that is located on a non-NXG Video-on-Demand server, such as the QuickTime/Darwin server, a Windows Media server, or a Helix Real server. This is valuable feature if you want to enter an off-network stream such as an MPEG-4 Stream from an Apple Darwin Server or if there is Windows Media or Real Networks content that needs to be displayed through the Portal Server interface.



URL	Enter a valid URL or IP address. For example:
	`rtsp://ipaddress/programname`
	`mms://ipaddress/videoname.wmv`

Type	Choose MPEG-1, MPEG-2, MPEG-4, MPEG-4 NXG, Document, WM, or Other. If you are creating a URL for stored video that points to `www.yahoo.com`, for example, select Document in this field—not Other. Select WM for .swf Flash streams.
Title	This is what will display to clients in the ETV Portal Server viewing pages
Folder	This is the folder on the VOD server in which the video will be displayed.
Keywords	Enter keywords that can be searched from the user interface.
Max. Concurrent Users	Set the maximum number of concurrent viewers for this stream to unlimited or any number greater than zero.

Press **Add** to add the VOD content to the list. VOD content also can be Modified or Deleted. Simply select the VOD content, make modifications (if required), and click **Modify** or **Delete**.

© 2007 VBrick Systems, Inc.

Add Non-VOD Content

PC Users Only. In the **VoD Content** section, administrators can also link to external documents such as PDF files, PowerPoint files, web pages, or anything that can be displayed in a browser or other external program. For content that needs to run with a specific application (for example, PowerPoint slides), the application must be present on the desktop for that file to be viewed. Use the content **Type** field to identify the content. Select a stream type (MPEG-1, MPEG-2, etc.) to add video content from an outside source. Select type **Document** for PDFs or Word documents, or type **Other** for PowerPoint presentations, Flash demos, etc. Each content type has a different icon on the **Video Library** page.

The URL must point to a web server or a local drive. The Portal Server server can act as the web server for this content, if the content is placed in the `c:\program files\vbrick\mcs` directory on the ETV Portal Server (or in any subdirectory you create, e.g. `... mcs\test_files\test.doc`). A local path or network shared path also can be entered. Content accessed from a local drive (or network shared path) needs to be entered in the format `c:/path/file` (it will fail if you use back slashes, for example `c:\path\file`). Also, this drive needs to be accessible by those that have access to the link.

Emergency Broadcast

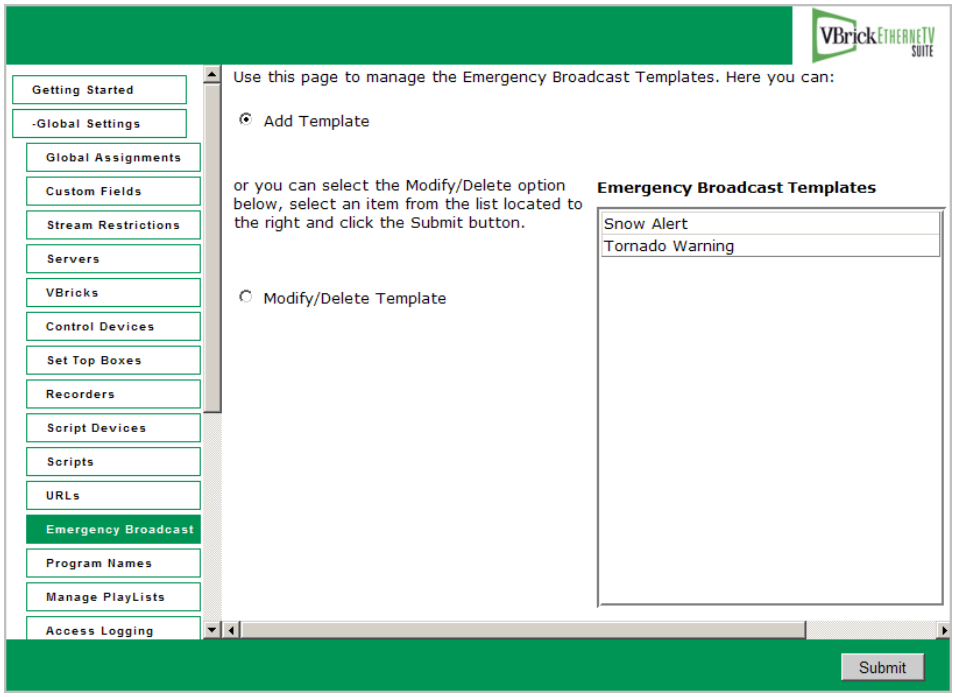
These pages are used to create emergency broadcast templates that Portal Server users can subsequently use to launch an emergency broadcast. *Emergency broadcasts are launched from the Portal Server user interface—not from the Admin console.* An emergency broadcast is a schedule that can be executed by Portal Server users with appropriate permissions. This schedule broadcasts a live or stored video to specified VBricks or set top boxes in case of an emergency. The schedule is executed instantly, for a specified duration or indefinitely. When done (or manually stopped) all preempted schedules automatically resume.

An emergency broadcast template pre-defines all parameters for the broadcast so that it can be launched immediately; it pre-empts all other broadcasts. Very simply, you define the source stream (live or stored) and the downstream targets (VBricks or STBs) and then save the template for future use. It is important to note that emergency broadcast streams are shown only on monitors or TVs attached to VBricks and STBs respectively. *They are not shown on the Portal Server user interface.* If you are watching a stream in the embedded player on the user interface browser, you will not see an emergency broadcast.

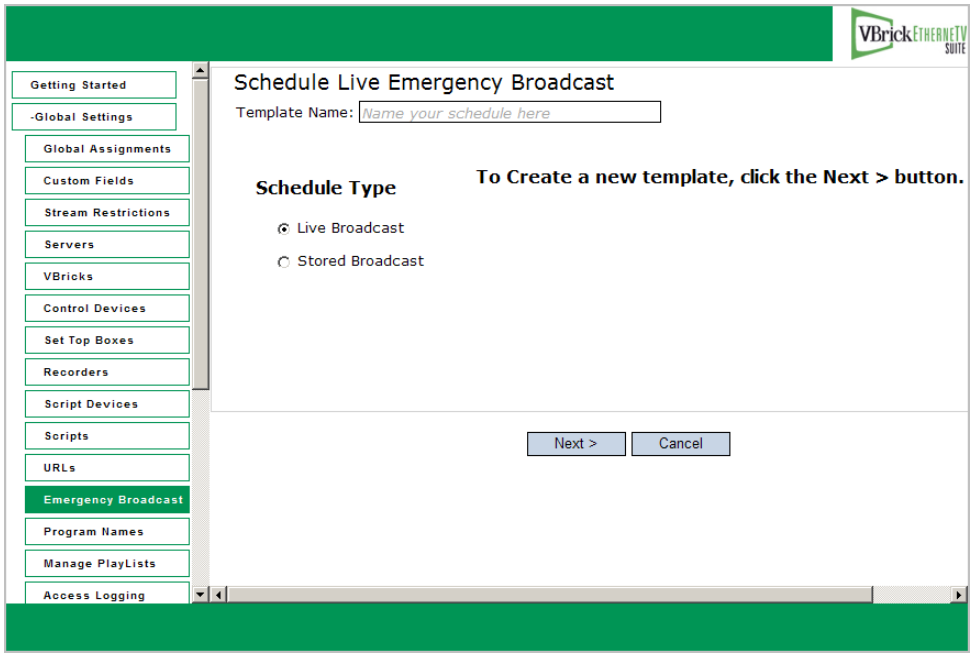
Note Live and stored broadcasts, in this context, refer to content that is being streamed over your IP multicast-enabled network. This does not mean there is IP broadcasting to your entire network.

▼ To create an Emergency Broadcast Template:

1. Go to **Global Settings > Emergency Broadcast**. This page shows a list of previously defined templates (if any).



2. Select **Add Template** and click **Submit** to display the following window.



3. Enter a **Template Name**, select a **Schedule Type**, and click **Next**. (Duplicate template names are allowed but not recommended.)

   Each **Schedule Type** subsequently has a different wizard depending on the selections you make but basically, you select the video source (which can be a live or stored broadcast), the downstream targets (VBricks or STBs) to which it will be broadcast, and configure any **Advanced Settings** (see note below) for the VBricks or STBs. When done the template you created is available to authorized Portal Server users as an Emergency Broadcast template. See the *ETV Portal Server User Guide* for more information.

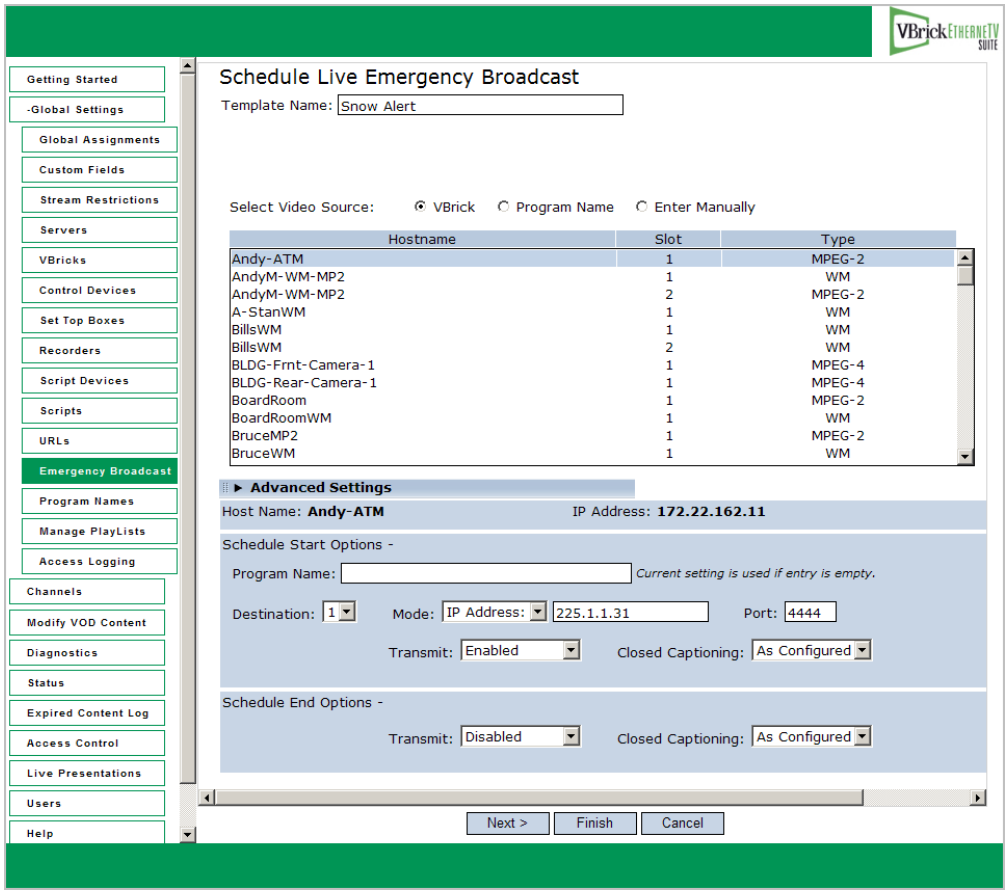
© 2007 VBrick Systems, Inc.

Note **Advanced Settings** are available to configure VBricks and STBs with exceptional configuration parameters. It is unlikely you will ever need to change these settings. In all cases you can safely ignore the **Advanced Settings** and use the defaults provided by ETV Portal Server.

Template name	Alphanumeric characters or spaces. No special characters.
Schedule Type	Live Broadcast • VBrick – Select a live stream by VBrick Name. Then select the destination VBricks or STBs. • Program Name – Select a live stream by Program Name from all available. Then select the destination STBs. • Enter Manually – Select an MPEG source residing at a specified IP address. Then select the destination STBs.
	Stored Broadcast • VoD Name – Select a VOD server and a source video. Then select the destination VBricks or STBs. • VBrick Name – Select a VBrick (or VBStar) and a source video. Then select the destination VBricks or STBs.

4. Configure **Advanced Settings** for VBricks and STBs as necessary. As noted, it is unlikely you will ever need to change these settings. In all cases you can safely ignore these settings and use the defaults provided by the Portal Server.

   These settings generally set configuration options for source devices and destination devices (VBricks and STBs) so that they are configured properly (e.g. transmit/receive enabled/disabled) at the beginning and end of an emergency broadcast. All required devices must be present and enabled for a successful emergency broadcast. The settings differ depending on the device (e.g. MPEG-1, MPEG-2 or MPEG-4) you select and may include some or all of the fields explained below.

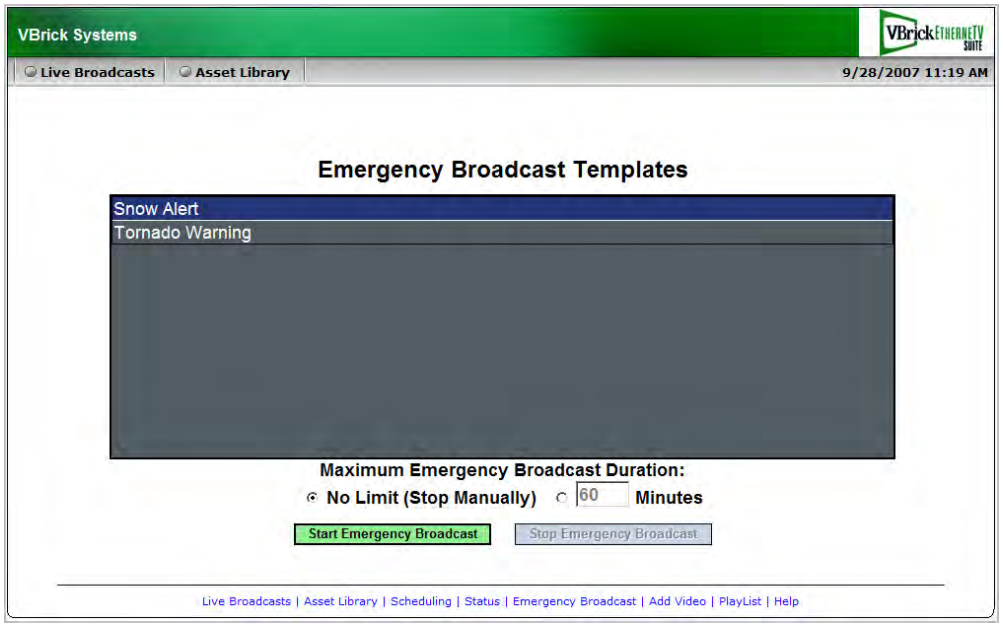


Schedule Start Options	Enter values that describe the device state at schedule start. • Program Name – Program name selected above. • Template – MPEG only. Screen varies for MPEG-1, 2, or 4. • Destination – Destination 1, Destination 2, RTSP Server. • Destination Address – Enter value. • Video Port – Enter value. • Audio Port – Enter value. • Closed Captioning Port – Enter value. • Video – Enabled, Disabled, As Configured. • Audio – Enabled, Disabled, As Configured. • Closed Captioning – Enabled, Disabled, As Configured.
Schedule End Options	Enter values that describe the device state at schedule end. • Video – Enabled, Disabled, As Configured. • Audio – Enabled, Disabled, As Configured. • Closed Captioning – Enabled, Disabled, As Configured.

5. Click **Next** to page through each wizard.
6. Click **Finish** when done.
7. Verify the information and click **Create Schedule** when prompted (or use the **Back** button to make changes). When finished, the template is added to the list of Emergency

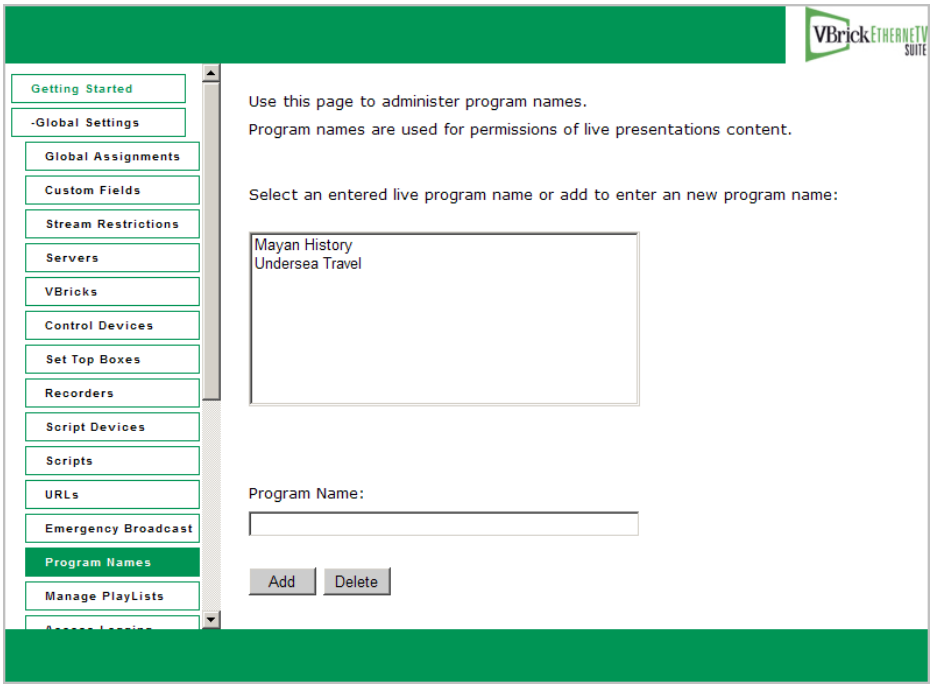
© 2007 VBrick Systems, Inc.

Broadcast Templates available to ETV Portal Server users from the Portal Server application. See the *ETV Portal Server User Guide* for more information.



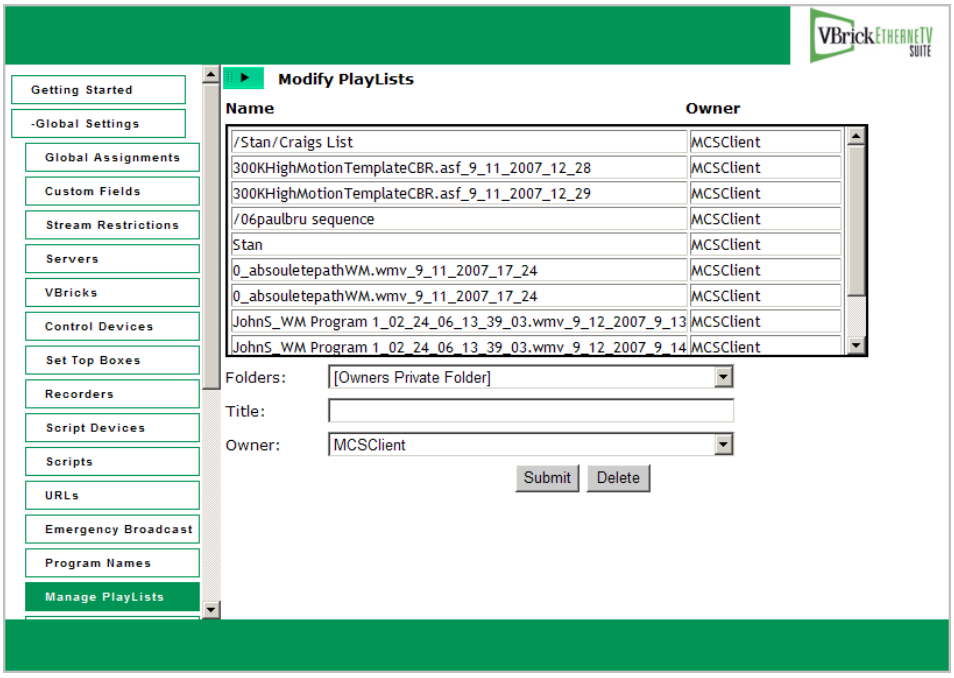
Program Names

Program Names are used with live presentations. A **Program Name** is the title that will be displayed on the **Live Broadcasts** page during a live, rich media presentation—if users have Live Channel privileges. Program names are also used to set permissions for live presentations and all defined Program Names are displayed in the **Add/Modify Live Channel Privileges** window. You can allow or deny viewing of any presentation by adjusting privileges in this window. A **Program Name** (e.g. HR Presentation) can be pre-configured (with permissions) in advance for use with VBPresenter. When you use this same name in the **MCS Program Name** field in VBPresenter for example, HR Presentation will be displayed on the Portal Server's **Live Broadcasts** page. See Configuring for Live Presentations on page 115 for more about program names.



Manage Playlists

Use this window to change playlist attributes including **Folder**, **Title**, and **Owner**. If Access Control is not enabled, the owner for all playlists defaults to MCSClient. Note that if Access Control is subsequently enabled, any previously created playlists will not be available unless they are re-assigned from MCSClient to other valid users.



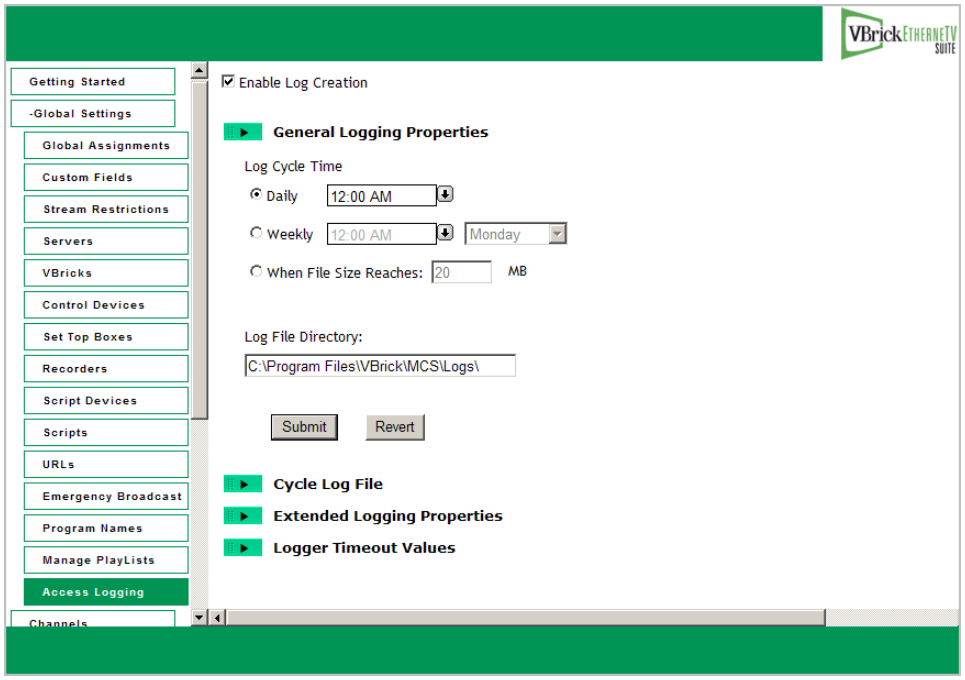
© 2007 VBrick Systems, Inc.

Folders	Select a folder location for the playlist. The default folder is the private MyMedia folder of the playlist owner.
Title	Use any alphanumeric characters *except* ' ^ : * ? | [ ] ( ) < > % #
Owner	The owner is the logged-in user who created the playlist.

Access Logging

Access logging tracks Portal Server usage. It creates logs that let you review who has watched what content, when, and for how long. Specifically, it logs access to live or VOD content, and to user-initiated recordings. **There are two output logs; one is used for live/VOD content and the other is for recordings.** The logs are created in a standard format and can be viewed with a customized template (see Viewing the Access Logs on page 62) or with log analysis tools like Web Log Explorer. Use the various configuration options described below to save the logs to a different computer, set log time periods, etc. By default, access logging is set to off and the logs are saved in Program Files\VBrick\MCS\Logs. *Note that log entries are written to the log file only after viewing or recording is complete.* To see what is *currently* being viewed or recorded, open the Logged Programs table in MCS using MySQL Query Browser or a similar tool. (MySQL Query Browser is available free of charge with the free software/open source GNU General Public License at http://www.mysql.com.) Be aware that the access logger has certain constraints; for example, it:

- does not log web page access. This is an IIS function that can be set and controlled by system administrators.
- does not work with the Apple QuickTime player.
- does not have a built-in parser. The logs can be viewed as text files or can be managed and viewed using third-party reporting and analysis tools.

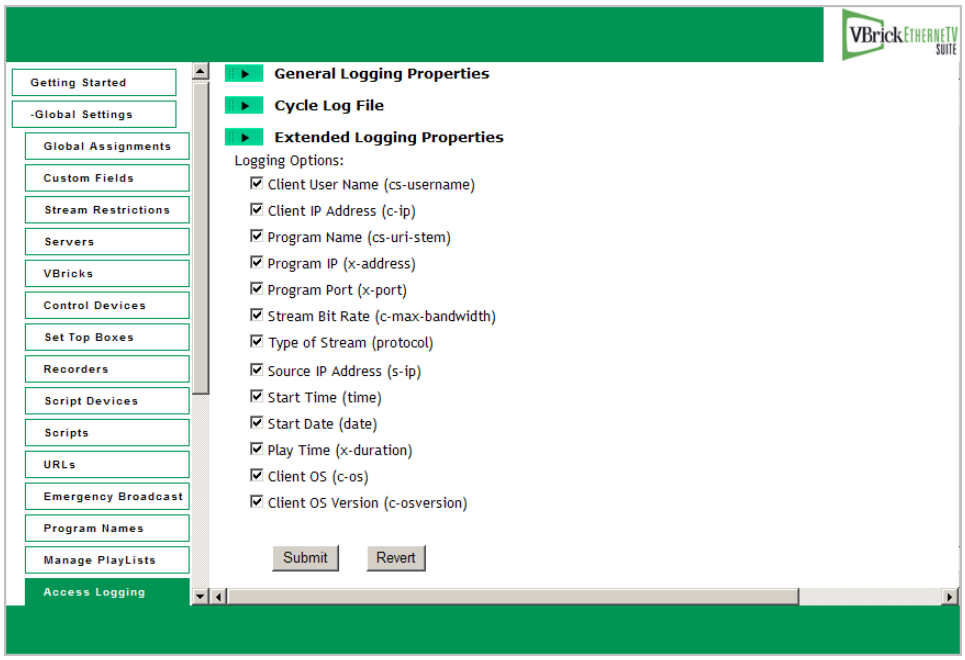


Enable Access Logging	Sets access logging on or off. Default = off.

Log Cycle Time	New log files can be created daily, weekly, or when the file reaches a certain size. Old files are never deleted or written over.
Log File Directory	Specifies where the log files are saved. This can be on the same machine as the Portal Server or on a different machine in the same network.
Cycle Log File	Click **Cycle Now** to close the existing log files and create new files.
Extended Logging Properties	See Extended Logging Properties below. Determines what fields are logged.
Logger Timeout Values	The timeout values (default two hours for stored content, four hours for live content) are typically used when a client machine crashes or hangs.

Extended Logging Properties

Use the following window to specify which fields are logged. The items in parentheses (e.g. cs-username) refer to the header field shown in the actual log file (see Figure 10 below). The fields are self-explanatory and most are standard W3C fields. (See http://www.w3.org/TR/WD-logfile.html for more about W3C log file formats.) Note that the fields used in each log will vary slightly and unused fields are marked with a hyphen "-". Note that the following non-standard fields may be incompatible with some reporting tools and can be de-selected: x-address, x-port, and x-duration. For best results with log analysis tools, do not de-select any other fields.



Viewing the Access Logs

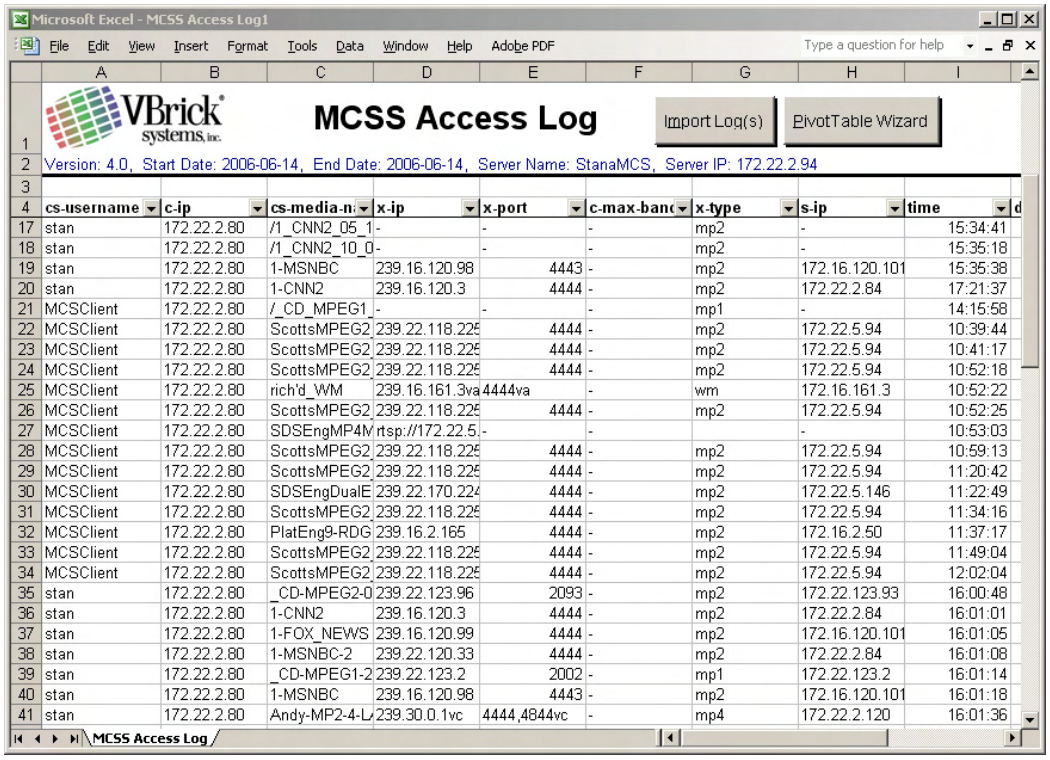
The log files are saved in Program Files\VBrick\MCS\Logs.You can view these file using a standard editor like Notepad or you can use the Excel spreadsheet template provided by VBrick. The MCSS Access Log.xlt template file makes to easy to view and sort log files. You can also use this template to build Pivot Tables to analyze the log data in greater detail. Pivot Tables are a powerful tool used to analyze multi-dimensional data. Pivot Tables are beyond

© 2007 VBrick Systems, Inc.

the scope of this document and are not explained here. For an introduction to Pivot Tables, there are a variety of resources on the web including the Microsoft Office online demo at http://office.microsoft.com/en-us/assistance/HA011989031033.aspx

▼ To create a pivot table:

1. Navigate to C:\Program Files\VBrick\MCS\Utils and double-click MCSS Access Log.xlt
2. When prompted, select **Enable Macros**.
3. Click **Import Log(s)** and navigate to the log files in Program Files\VBrick\MCS\Logs
4. Select one or more log files by holding down the **Ctrl** or **Shift** keys while selecting files.
5. Once the window is populated with log data (Figure 10) you can view or sort any of the columns as necessary.
6. Click **Pivot Table Wizard** and follow the prompts to build a Pivot Table.


Microsoft Excel - MCSS Access Log1
File Edit View Insert Format Tools Data Window Help Adobe PDF
Type a question for help
MCSS Access Log
Import Log(s)
PivotTable Wizard
Version: 4.0, Start Date: 2006-06-14, End Date: 2006-06-14, Server Name: StanaMCS, Server IP: 172.22.2.94
MCSS Access Log

	cs-username	c-ip	cs-media-n	x-ip	x-port	c-max-ban	x-type	s-ip	time
17	stan	172.22.2.80	/1_CNN2_05_1	-	-	-	mp2	-	15:34:41
18	stan	172.22.2.80	/1_CNN2_10_0	-	-	-	mp2	-	15:35:18
19	stan	172.22.2.80	1-MSNBC	239.16.120.98	4443	-	mp2	172.16.120.101	15:35:38
20	stan	172.22.2.80	1-CNN2	239.16.120.3	4444	-	mp2	172.22.2.84	17:21:37
21	MCSClient	172.22.2.80	/_CD_MPEG1_	-	-	-	mp1	-	14:15:58
22	MCSClient	172.22.2.80	ScottsMPEG2	239.22.118.225	4444	-	mp2	172.22.5.94	10:39:44
23	MCSClient	172.22.2.80	ScottsMPEG2	239.22.118.225	4444	-	mp2	172.22.5.94	10:41:17
24	MCSClient	172.22.2.80	ScottsMPEG2	239.22.118.225	4444	-	mp2	172.22.5.94	10:52:18
25	MCSClient	172.22.2.80	rich'd_WM	239.16.161.3va	4444va	-	wm	172.16.161.3	10:52:22
26	MCSClient	172.22.2.80	ScottsMPEG2	239.22.118.225	4444	-	mp2	172.22.5.94	10:52:25
27	MCSClient	172.22.2.80	SDSEngMP4M	rtsp://172.22.5.	-	-		-	10:53:03
28	MCSClient	172.22.2.80	ScottsMPEG2	239.22.118.225	4444	-	mp2	172.22.5.94	10:59:13
29	MCSClient	172.22.2.80	ScottsMPEG2	239.22.118.225	4444	-	mp2	172.22.5.94	11:20:42
30	MCSClient	172.22.2.80	SDSEngDualE	239.22.170.224	4444	-	mp2	172.22.5.146	11:22:49
31	MCSClient	172.22.2.80	ScottsMPEG2	239.22.118.225	4444	-	mp2	172.22.5.94	11:34:16
32	MCSClient	172.22.2.80	PlatEng9-RDG	239.16.2.165	4444	-	mp2	172.16.2.50	11:37:17
33	MCSClient	172.22.2.80	ScottsMPEG2	239.22.118.225	4444	-	mp2	172.22.5.94	11:49:04
34	MCSClient	172.22.2.80	ScottsMPEG2	239.22.118.225	4444	-	mp2	172.22.5.94	12:02:04
35	stan	172.22.2.80	_CD-MPEG2-0	239.22.123.96	2093	-	mp2	172.22.123.93	16:00:48
36	stan	172.22.2.80	1-CNN2	239.16.120.3	4444	-	mp2	172.22.2.84	16:01:01
37	stan	172.22.2.80	1-FOX_NEWS	239.16.120.99	4444	-	mp2	172.16.120.101	16:01:05
38	stan	172.22.2.80	1-MSNBC-2	239.22.120.33	4444	-	mp2	172.22.2.84	16:01:08
39	stan	172.22.2.80	_CD-MPEG1-2	239.22.123.2	2002	-	mp1	172.22.123.2	16:01:14
40	stan	172.22.2.80	1-MSNBC	239.16.120.98	4443	-	mp2	172.16.120.101	16:01:18
41	stan	172.22.2.80	Andy-MP2-4-L	239.30.0.1vc	4444,4844vc	-	mp4	172.22.2.120	16:01:36

Figure 10. Imported Access Log

© 2007 VBrick Systems, Inc.

Chapter 3

Server Administration

Topics in this chapter

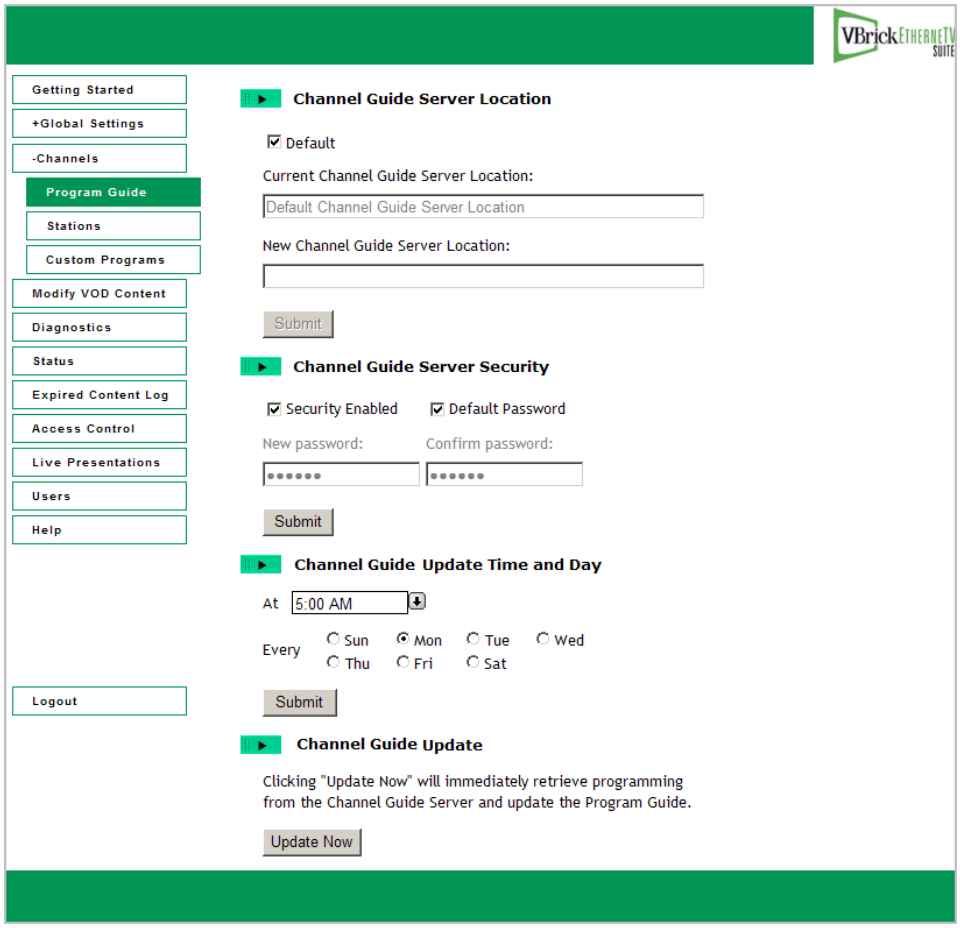
Channels 65
Modify VOD Content 73
Diagnostics 75
Status 75
Expired Content Log 76
Access Control 76
Live Presentations 83
Users 84
User Groups 84
Resource Groups 84
Help 84
Logout 85

Channels

Channel Guide

This page is used to define the location and update parameters for the Channel Guide Server. This server is typically a VBrick Apache machine that can be used to connect to a third-party content provider. In this type of scenario, the third-party provider provides *programming* data that is shown on the user interface in the Channel Guide. This functionality requires a Channel Server license. If this license is not installed, the options for server **Location** and **Security** (password) are not shown on the following page.

Note VBrick has partnered with a leading content provider, to provide news, information, and entertainment programming for the Portal Server. This is optional service that requires a license and may not be supported at your site.



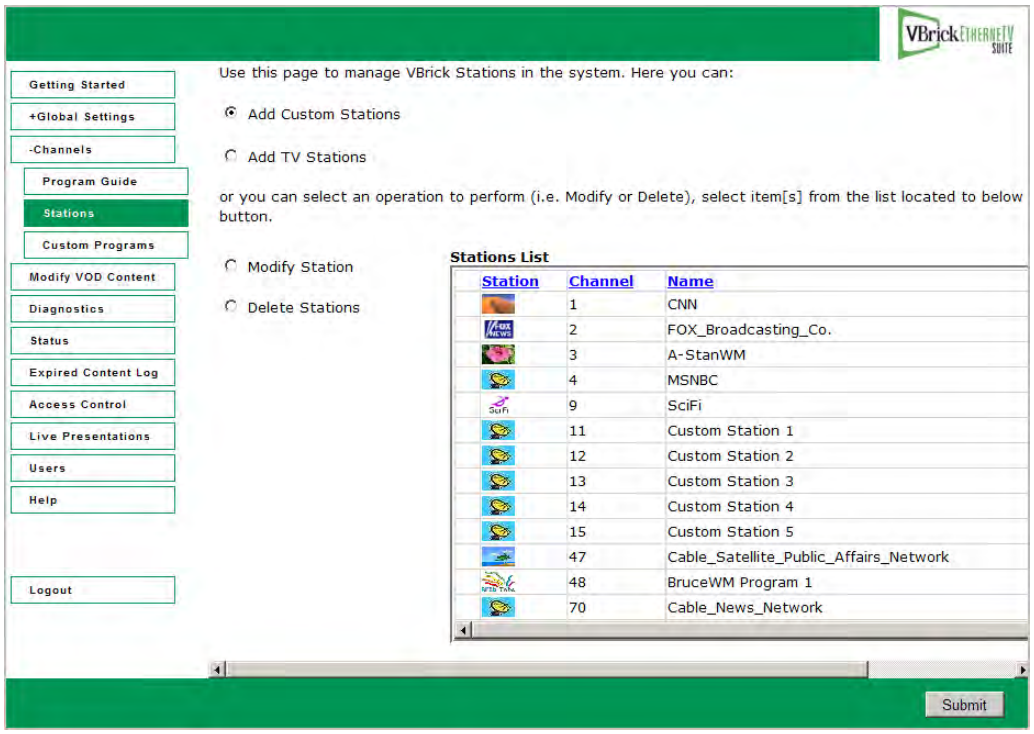
Channel Guide Server Location	The location of the VBrick Channel Guide Server. To enter a different location, uncheck the **Default** box and enter a valid URL in the following format: http://www.<server_ip_address>.
Channel Guide Server Security	By default, password security is enabled. Uncheck to disable, and then enter and confirm a different password.
Channel Guide Update Time and Day	Select the time and day when the Portal Server will connect to the specified Channel Guide Server for program updates. This updates the Channel Guide on the user interface. When *TV Station* program data is updated, all expired *Custom Station* program data (more than 14 days old) is purged.
Channel Guide Update	Click **Update Now** to immediately retrieve programming from the Channel Guide Server and/or update the Channel Guide on the user interface. An update purges all outdated programming information from the database.

Stations

Use this page to add stations to the Channel Guide on the Portal Server "user" interface. There are two types of stations. **Custom Stations** are those for which *you* define program information and associate with a stream. **TV Stations** are those acquired through a third-party provider. **TV Stations** are also associated with a stream and already have program information

© 2007 VBrick Systems, Inc.

provided by a Channel Guide Server. Note that the **Add TV Stations** option is not shown unless you have a Channel Guide Server license installed on the Portal Server (see Portal Server License Files on page 14 for more information). All currently defined stations are shown in the **Stations List**.



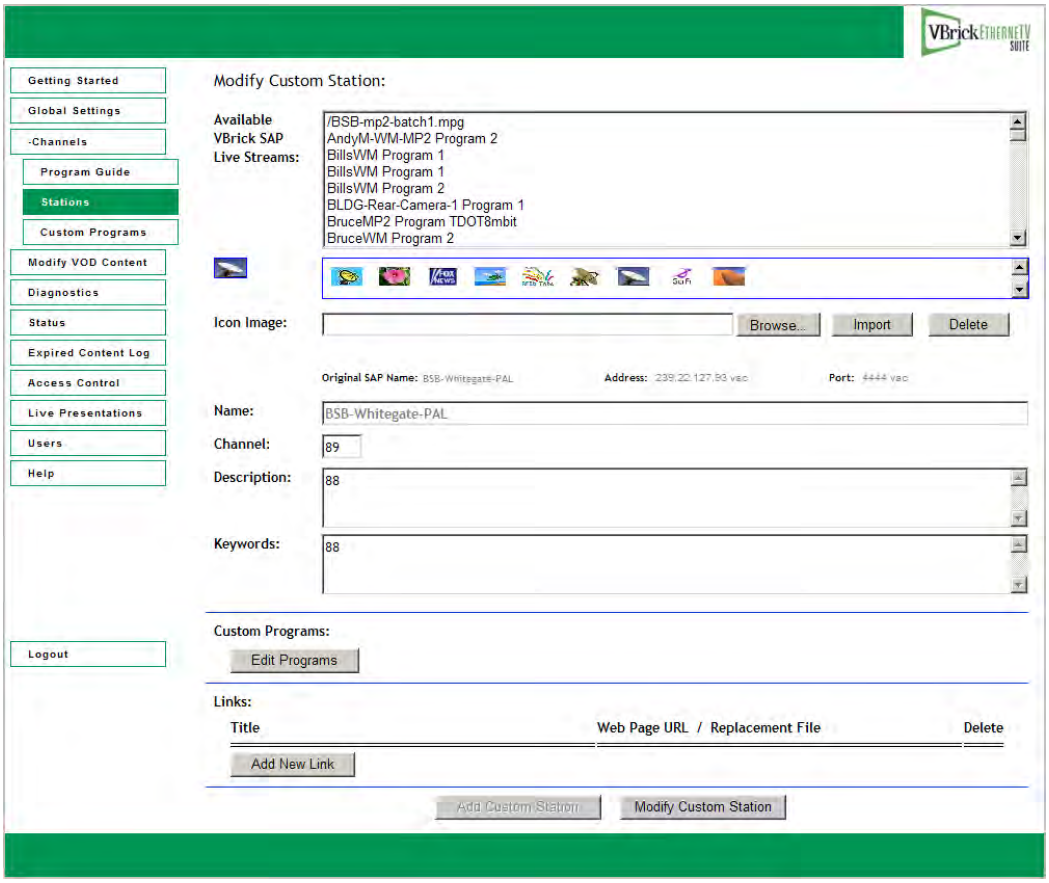
The Portal Server discovers all available live streams on the network. On a network with many live streams, the administrator can keep the stream list organized by assigning channel numbers. This also provides an environment for end users that is similar to television. When adding stations, you can assign or change the **Icon**, **Name**, **Channel** number etc. You can also enter a searchable **Description** that displays in the **View Info** popup when you mouseover the channel number in the user interface. You can also enter **Keywords** for searching, and values for any custom fields that have been defined (see Custom Fields on page 25).

Note For best viewing results after adding stations, click the **Live Broadcasts** button on the user interface to refresh the page and verify your changes. To avoid caching conflicts, do not use the browser refresh (F5) button.

Add Custom Stations

▼ To add a custom station:

1. Go to **Channels > Stations** and click **Add Custom Stations**.
2. Click on any *available* live stream to populate the window shown below. Note that only those streams not currently assigned to stations are displayed and available for use.



3. Select an existing icon or **Browse** to a file and select **Import** to make additional icons available.
4. Change the station **Name** (optional) and enter a **Channel** number (required).
5. Add a **Description** of the channel and **Keywords**. These are displayed on the **Info** page shown when you mouseover the station icon. They are associated with the stream and make it easier to search for specific content.
6. When done click **Add Custom Station**. This creates the station, disables the **Add Custom Station** button, and enables the **Edit Programs** and **Add New Links** buttons.
7. Add custom programming information (see Custom Programs) and links (see Add New Links) as explained below.
8. Click **Modify Custom Station** when done to save your changes.

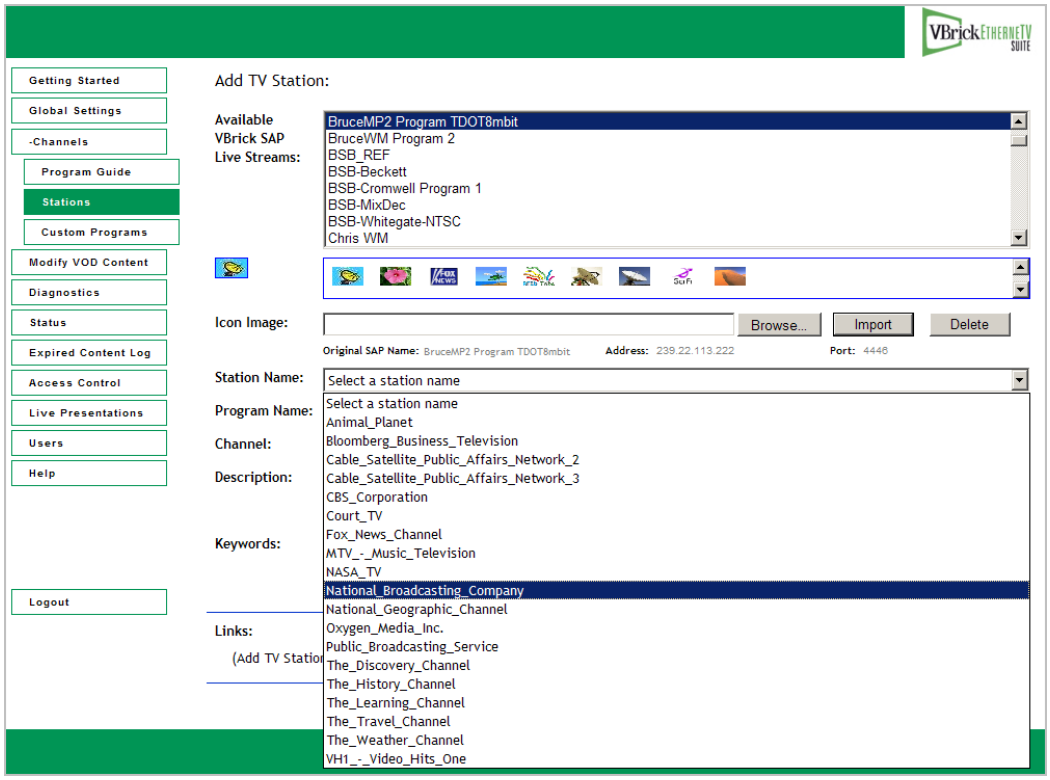
Available VBrick SAP Live Streams	Select an available live stream on your network. These were previously created and include VBrick SAPs (Session Announcements), multicasts from VOD servers, and URLs that were manually entered. See URLs on page 52 for more information about manually-entered URLs. *Note that only those streams not currently assigned to stations are displayed in this list.*
Icon Image	Navigate to any valid image file (.jpg, .gif, or .png, only). Use an image that will scale appropriately. All images are resized to 18x30 px.

© 2007 VBrick Systems, Inc.

Name	Required. Name assigned to the station that will display on the popup when you mouseover the icon on the Live Broadcasts page.
Channel	Required. Unique number that will display on the popup when you mouseover the icon on the Live Broadcasts page
Description	Optional. Description that will display on the View Info page.
Keywords	Optional. Enter searchable keyword(s) separated by commas or spaces that will display on the View Info page.
Custom Programs	Lets you add custom programming data. Note that you must add a Custom Station before creating programs for it.
Links	Optional. Add hyperlinks that will display on the View Info page. See Add New Links below. Note that you must add a Custom Station before creating links for it.

Add TV Stations

This option is not shown unless you have a license for a Channel Guide Server. If you do have a license, certain content is being made available from a third-party provider. Adding a **TV Station** is the same as adding a **Custom Station** (see above) with two important distinctions. First, you must select a **Station Name** from the pre-populated list, an example of which is shown below. Second, there is no button that will allow you to create custom programming. The programming for TV Stations is automatically provided by the specified Channel Guide Server and updated at regular specified intervals (see Channel Guide on page 65 for details).

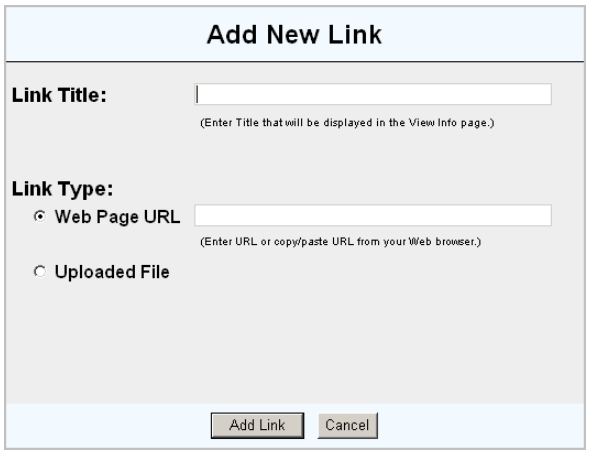


Add New Links

This feature lets you add a hyperlink to the page you get by clicking the **View Info** link that is associated with each live stream.

▼ To add a new link:

1. Click **Add New Link** and enter a **Link Title** and **Link Type**.
2. Enter a Web Page URL or navigate to an upload file (an image, a Microsoft Word document, etc.).
3. Click **Add Link** when done and repeat as many times as necessary.



Link Title	The title actually displayed on the View Info page, for example "Additional Information."

© 2007 VBrick Systems, Inc.

Link Type	• Web page URL – Enter a valid URL or copy and paste one from your web browser. • Uploaded File – Browse to select an upload file. This can be a PowerPoint, an image, or any file you want to make available to end users. The file is automatically uploaded to the Portal Server and the Portal Server creates a URL for end users to access it.

Custom Programs

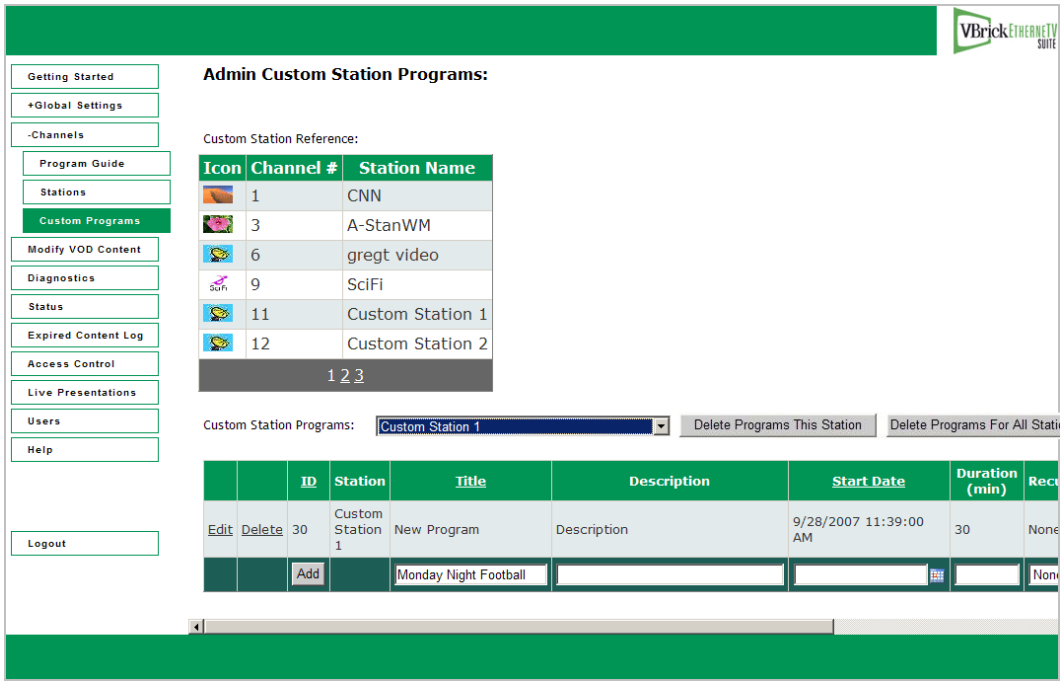
This page is used to add programming information to an existing station. You can only program custom stations; TV stations (if present) are auto-programmed by a Channel Guide Server. You use the **Custom Programs** page to manually create programming data and associate it with a Custom Station. For example, you may want to modify the Channel Guide so that "Monday Night Football" is shown in the 8–10 P.M. time slot on Monday nights from September through January.

Add Custom Programs

▼ To add custom programming to a custom station:

1. Click on **Custom Programs** to display the Custom Stations page.
2. The Custom Station Reference list shows all currently defined *custom* stations. Select a Custom Station from the dropdown list (below the Reference pane) and click **Add New Custom Program**.
3. Use the fields explained below to create custom programming for the selected station. Click on the header titles as appropriate to sort the entries in the list.
4. Use the horizontal slider bar to display all fields. When done, click **Add**. The program will be added to the specified time slot and you will see a view similar to Figure 11 when you mouseover the item in the Channel Guide on the user interface.

Note When *TV Station* program data is updated from the Channel Guide Server, all expired *Custom Station* program data (more than 14 days old) is purged.



Custom Station Programs	From the dropdown list, select a defined Custom Station for which you want to define a program.
Delete Programs This Station	Delete all programming data for the *selected* station.
Delete Programs For All Stations	Delete all programing data for *all* stations.
ID	Program ID. Read only.
Station	Station Name. Read only.
Title	This is the title shown in the Channel Guide, for example "Monday Night Football."
Description	This is the description shown on the popup (see Figure 11) when you mouseover the item in the Channel Guide and click Info.
Start Date	Use the calendar to select the start date and start time. Alternately, you can manually enter the values in the proper format: for example: 9/10/2007 5:30:00 PM
Duration	Required. Program length in minutes.
Recurrence	None | Daily | Weekly. If weekly, occurs on the same *day* as specified in Start Date.
End	Select NoEnd or EndDate and use calendar.
Recur End Date	Use the calendar to select recurrence end date.

© 2007 VBrick Systems, Inc.

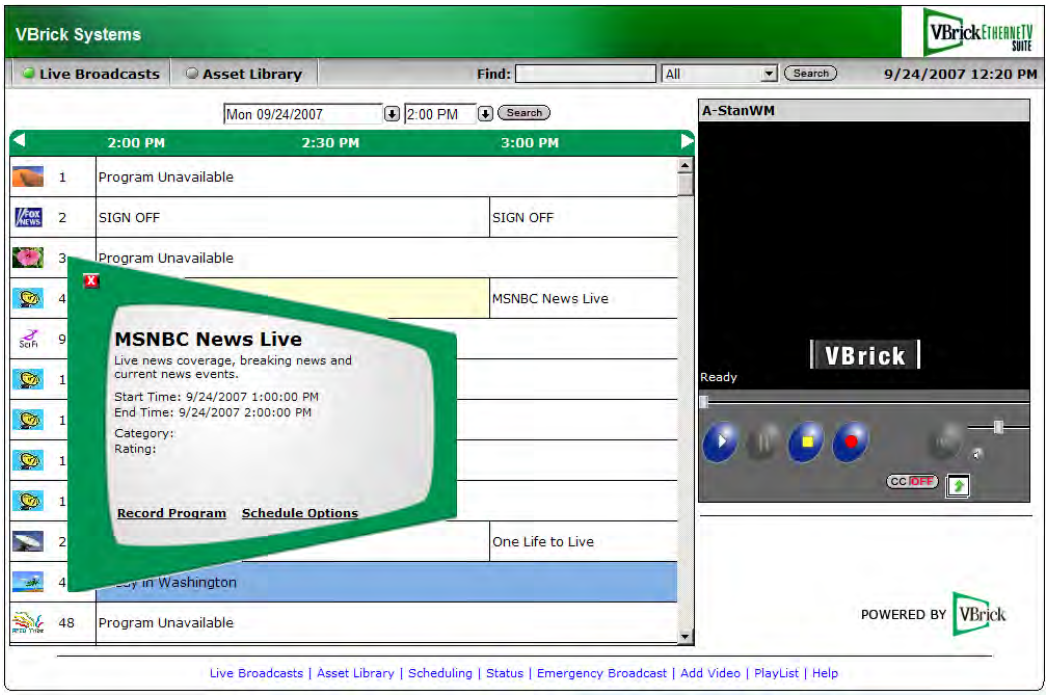


Figure 11. Custom Program Data

Note The message "Program Unavailable" in the Channel Guide means there is no programming data associated with the stream. *It does not mean the stream itself is unavailable.* You can still click on the stream to launch it in the preview window.

Edit Custom Programs

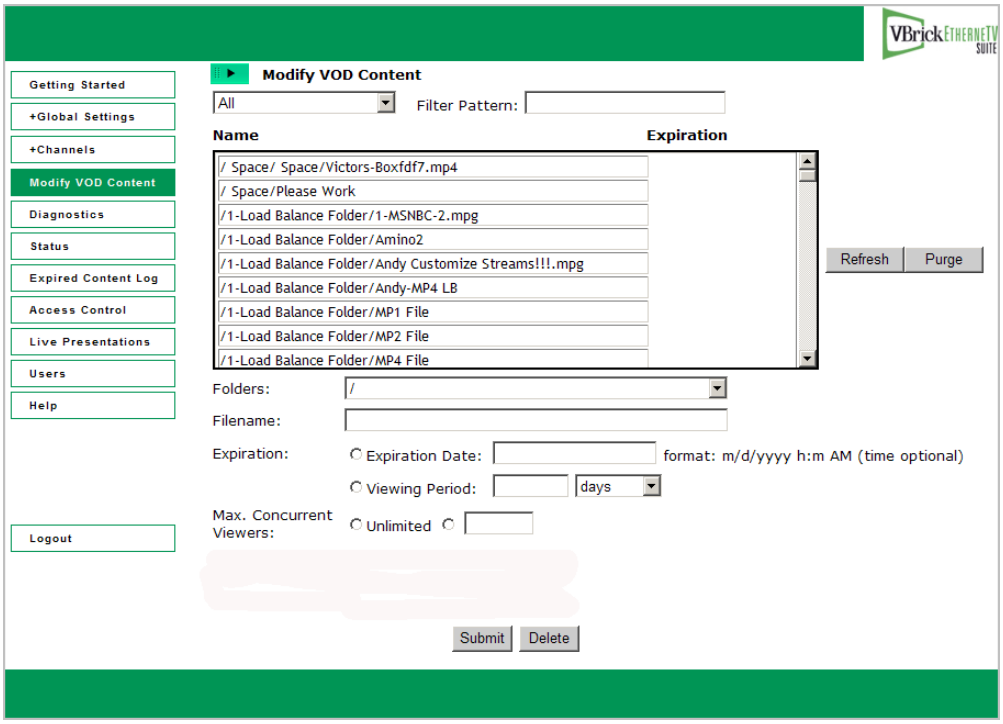
▼ To edit a Custom Program:

1. Navigate to the program you want to change and click **Edit**.
2. Manually edit any of the fields as necessary and click **Update** when done.

Modify VOD Content

Video on Demand Servers only. Administrators and authorized users can modify and delete content located on their video on-demand servers. (Note that you cannot delete or modify any content files that are currently in use.) Administrators can find or filter the displayed assets by clicking on **All**, **Keyword**, **Title**, or **Expiration Date**. You can also use this window to set **Expiration** and to define the maximum number of concurrent viewers for a stream. Also, be aware that a user with publishing permissions can delete content by clicking the **Info** hyperlink and then **Delete Video**. To disable this user option, disable the user's content publishing permissions (see Allow Content Publishing on page 96).

Note NXG1 only. You cannot rename or otherwise manage VOD files stored on some legacy NXG1 servers. This feature is supported on all NXG2 servers and on all other servers currently available with ETV Portal Server.



Search box (All)	Search for specific assets by selecting All, Keyword, Title, or Expiration Date. Then click Refresh.
Filter Pattern	Search for specific assets using a filter pattern. Type any text string and click Refresh. For example, type mp4 to search for assets with mp4 in the title. The filter does not recognize "wildcards" and is not case-sensitive.
Name	Video content name. Click on Refresh to re-paint the screen or Purge button to remove the artifacts of failed Delete operations.
Expiration	Expiration date if any.
Folders	Use to navigate to a specific folder.
Filename	Click once on any named content in the list to populate this field.
Expiration	• Expiration Date – set date in mm/dd/yyyy 12:00 AM format. • Viewing Period – set a value for viewing period in hours, days, weeks, months, or years.
Max. Concurrent Users	Defines the maximum number of users who can view this stream at the same time. Select unlimited or enter a value greater than zero.

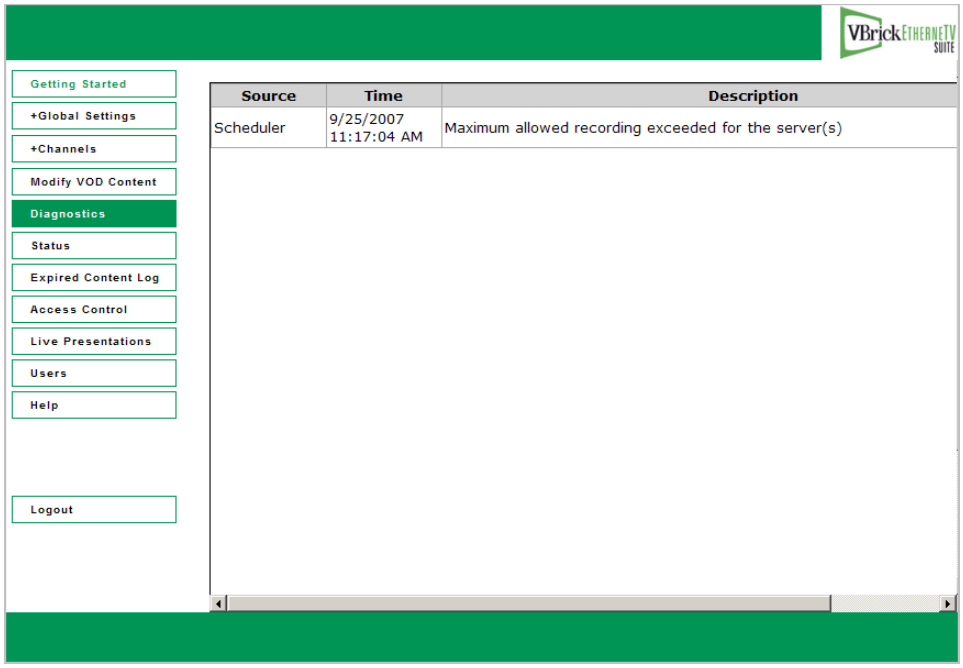
▼ To modify VOD Content:

1. Click on the content to be changed.
2. Enter a new filename and/or path for that file. Note that the file must be alphanumeric characters and cannot contain embedded spaces.
3. Set the **Expiration Date** or **Viewing Period** as necessary.
4. To delete a file, select the file and click **Delete**.

© 2007 VBrick Systems, Inc.

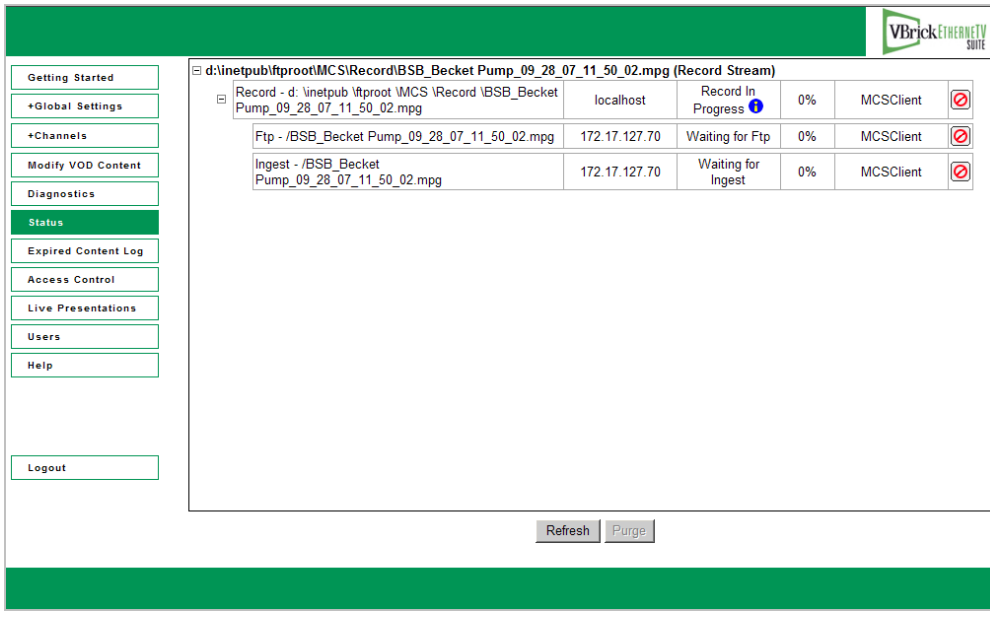
Diagnostics

This window displays information about Scheduler events only. It displays system log messages by source and time and (generally) IP address. Use **Clear All** to empty the log.



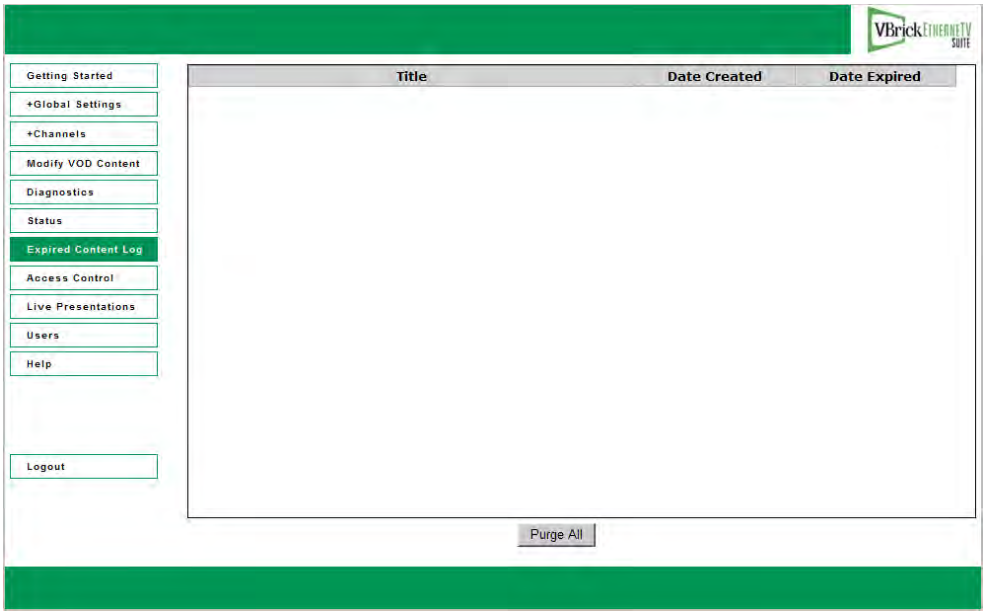
Status

This window shows the status of videos being added or recorded. Use **Refresh** and **Purge** as necessary. Use the tree controls on the left to expand (or contract) individual entries. Click the Cancel icon to the left of each to cancel a recording or ingestion in progress. This also cancels the recording on the **Live Broadcasts** page.



Expired Content Log

This window shows all expired content in chronological order with the oldest expiration date first. Click **Purge All** to delete all records in the log. See Modify VOD Content on page 73 and Stream Restrictions on page 26 for more information.



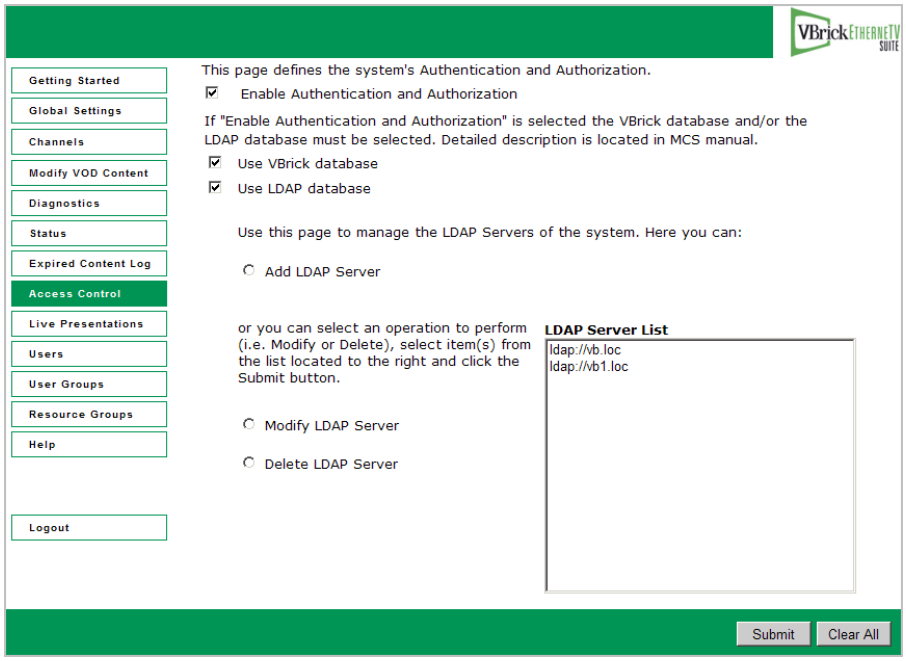
Access Control

Under the Access Control section, administrators have the ability to enable Authentication and Authorization which requires users to login and be authenticated. By default **Enable Authentication and Authorization** is unchecked which allows everyone to access all content and all functions (recording, publishing, etc.). When Access Control is enabled, **User Groups**, and **Resource Groups** are shown on the navigation bar. Access control determines what functionality is available to each user. For example some users may have unlimited access, while others can only view certain live channels and may not have permission to record live channels or add videos to the VOD server. Users and User Groups on page 87 explains in detail how configure users and groups.

Access control also lets you specify which folders are used when individual users record live broadcasts, add videos, or autoingest content. If you do not enable **Authentication and Authorization**, all of these actions default to the root folder (which can quickly get cluttered).

Note As soon as you check **Enable Authentication and Authorization**, users will be prompted for User Names and Passwords. VBrick recommends configuring the system prior to user access or during off hours when the network is idle.

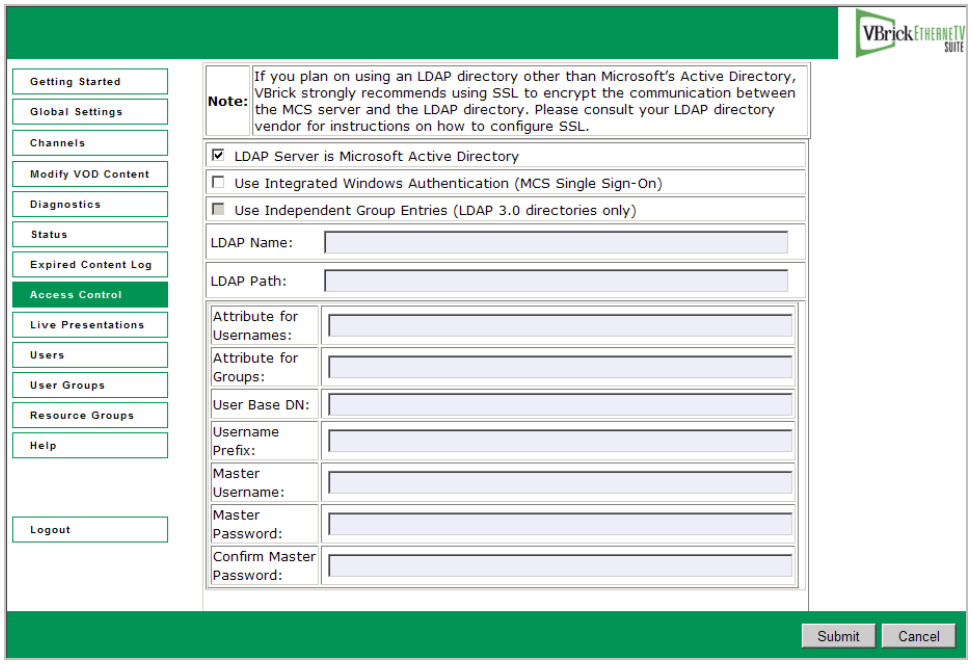
© 2007 VBrick Systems, Inc.


Getting Started
Global Settings
Channels
Modify VOD Content
Diagnostics
Status
Expired Content Log
Access Control
Live Presentations
Users
User Groups
Resource Groups
Help
Logout
This page defines the system's Authentication and Authorization.
Enable Authentication and Authorization
If "Enable Authentication and Authorization" is selected the VBrick database and/or the LDAP database must be selected. Detailed description is located in MCS manual.
Use VBrick database
Use LDAP database
Use this page to manage the LDAP Servers of the system. Here you can:
Add LDAP Server
or you can select an operation to perform (i.e. Modify or Delete), select item(s) from the list located to the right and click the Submit button.
LDAP Server List
ldap://vb.loc
ldap://vb1.loc
Modify LDAP Server
Delete LDAP Server
Submit
Clear All

Enable Authentication and Authorization	Enable authentication and authorization which requires users to login and be authenticated. If not checked, all users have access to all functionality and content.
Use VBrick database	Use the VBrick (non LDAP) database provided with ETV Portal Server.
Use LDAP database	Use an LDAP database. VBrick supports major LDAP vendors but only Microsoft Active Directory and Novell eDirectory are fully tested and supported.
Add/Modify/Delete LDAP Server	The Portal Server supports multiple LDAP servers. Use these options to add or manage LDAP servers.

Using LDAP Servers

Administrators have the option of using the onboard **VBrick database** for authentication, using an **LDAP database**, or using both. *VBrick supports major LDAP vendors but only Microsoft Active Directory, Novell eDirectory, and OpenLDAP are fully tested and supported.* If authenticating against Microsoft's Active Directory, check the **LDAP Server is Microsoft Active Directory** check box and enter the path to the LDAP server in the **LDAP Path** box. If authenticating against a directory other than Microsoft Active Directory, do not check **LDAP Server is Microsoft Active Directory**. LDAP (Lightweight Directory Access Protocol) is a standardized method to access directories from multiple vendors. A complete discussion of LDAP is beyond the scope of this document.



LDAP Server is Microsoft Active Directory	Check only if using Microsoft Active Directory.
Use Integrated Windows Authentication	Use "single sign-on." This means that once you login to your local network, you can open ETV Portal Server without re-entering your login credentials. See below Using Single Sign-On.
Use Independent Group Entries	If unchecked (the default), the user's group memberships are stored as attributes of the user's directory entry identified by the **Attribute for Groups** field. If checked, MCS will support LDAP models where group entries are independent of user entries. If checked, the Independent Group ObjectClass and Independent Group Identifier fields are required.
LDAP Path†	*Required by ETV Portal Server.* Case sensitive. Must begin with `LDAP://` Points to a specific position in the LDAP tree and also includes the machine IP address (or Domain name) on which the server is running. For example use `LDAP://myLDAPServer` with Microsoft Active Directory; use `LDAP://myLDAPServer:636` with Novell eDirectory. For more information, see Installing the Root Certificate on page 81.
Attribute for Usernames†	*Required by ETV Portal Server.* Attribute to identify a user. The following sample username attributes are widely used but refer to a specific LDAP schema: • Microsoft Active Directory: `sAMAccountName` • Novell eDirectory: `uid`

© 2007 VBrick Systems, Inc.

Attribute for Groups†	*Required by ETV Portal Server.* Attribute to identify the group to which a user belongs. The following sample group attributes are widely used but refer to a particular LDAP schema: • Microsoft Active Directory: `memberOf` • Novell eDirectory: `groupMembership`
User Base DN	Base distinguishing name (DN) of user nod and/or the Base DN for the Master Username.
Username Prefix	Used in non-Active Directory environments where the user name is prefixed with a specific string such as `uid=` or `cn=`. The following sample prefixes are widely used but refer to a specific LDAP schema: • `uid=` • `cn=`
Master Username	Required for single-sign-on. User name that has admin permission to browse the LDAP tree. Used to browse the LDAP tree to get user groups.
Master Password	Required for single-sign-on. Password for Master Username.
Ind. Group ObjectClass	A group attribute in the LDAP database. Identifies which entries will be searched for user memberships.
Ind. Group Identifier	The group attribute that uniquely identifies a group. MCS will match the values returned for this attribute with group names entered on the **User Groups** page.

† ETV Portal Server required field. All others are optional.

Note The Softerra LDAP Browser 2.6 provides an Explorer-like LDAP client you can use to browse the LDAP tree. It is available for Windows only and can be downloaded free of charge from Softerra at http://www.ldapbrowser.com

Using Single Sign-On

To use single sign-on, go to **Access Control** and then check **Enable Authentication and Authorization** and **Use LDAP Database**. If the LDAP server is Microsoft Active Directory, you can select **Use Integrated Windows Authentication** to enable "MCS Single Sign-on." This means that once you login to your local network with your assigned credentials, you can open ETV Portal Server without re-entering your login credentials. ETV Portal Server uses your assigned credentials to authenticate and authorize your defined permissions within the application. (If using an LDAP directory other than Microsoft's Active Directory, VBrick strongly recommends using SSL to encrypt the communication between the Portal Server server and the LDAP directory. Please consult your LDAP vendor documentation for instructions on how to configure SSL.) When configuring for Integrated Windows Authentication, keep the following points in mind:

- Integrated Windows Authentication is only valid when using LDAP Authentication with Microsoft Active Directory.
- You must perform an additional configuration step in IIS as explained below in Configuring IIS for Single Sign-On.

- Integrated Windows Authentication only works seamlessly with Microsoft Internet Explorer browsers (Windows and Macintosh). When accessing ETV Portal Server, you will get a popup login window *only* if you have not previously logged in to the network.
- When using Integrated Windows Authentication, all single-sign-on users must have an Active Directory account and the Portal Server must be part of the Windows domain.
- When using Integrated Windows Authentication, Microsoft Internet Explorer's default behavior is that it will *not* prompt for an ID/password when the server is in the **Local Intranet Zone**. (By default, Internet Explorer assumes a URL without a period (.). This means `http://yourserver/` is in the **Local Intranet Zone** while `http://yourserver.yourcompany.com` (or `http://199.88.7.11`)) is in the **Internet Zone**.

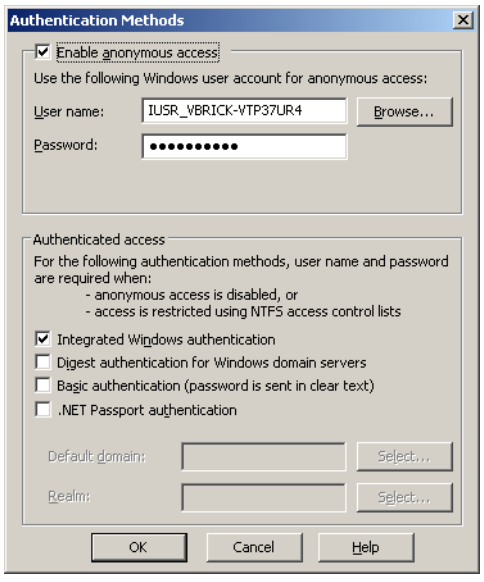
Note If single sign-on is enabled on multiple LDAP servers, when a user signs on for the first time, the system validates the login credentials against all servers configured for single sign-on. If you are validated by at least one server, you are automatically logged in. In most cases when single sign-on is enabled, the user will *not* be prompted for a **Domain** name at login.

Configuring IIS for Single Sign-On

Use the following steps to configure IIS for single sign-on. *If you do not perform these steps, the login page will likely be blank when you launch the Portal Server.*

▼ To configure IIS for single sign-on:

1. Go to **Start > Administrative Tools > Computer Management**.
2. Expand **Services and Applications** and expand **Internet Information Services (IIS) Manager**.
3. Expand **Web Sites** and then right-click on **Default Web Site** and select **Properties**.
4. Go to **Directory Security > Authentication and access control** and make sure that **Integrated Windows authentication** is checked on the following window.



© 2007 VBrick Systems, Inc.

Using Single Sign-On

▼ To use single-sign-on (and avoid username/password prompts), you must do **one** of the following:

- Access the Portal Server by the *alphabetical name* (for example `http://yourserver`).
- Access the Portal Server by the *IP address* in which case you must also add the Portal Server to the **Local Intranet Zone** (**Internet Options > Security > Sites**). This setting can be pushed company-wide by an administrator using security policies.

5. Change Internet Explorer's default settings to allow **Automatic logon with current username and password** (Go to **Internet Options > Security > Custom Level > User Authentication**).

Using LDAP Servers with SSL

Installing the Root Certificate

If the LDAP server requires SSL (Secure Sockets Layer) for encryption and authentication, you will need to install the certificate locally on the ETV Portal Server as a **Trusted Root Certificate Authority**.

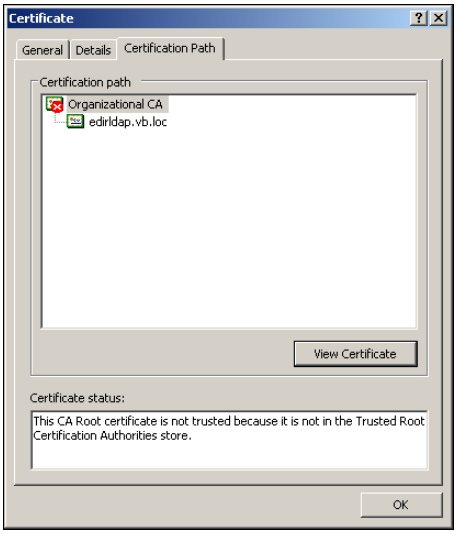
▼ To install the root certificate locally on the ETV Portal Server as Trusted Root Certificate Authority:

1. Open Internet Explorer.
2. In the address bar type `https://LDAPSERVER:636` where `LDAPSERVER` is the address of the LDAP Server associated with Certificate Authority (See Resolving Other Security Alerts on page 83) and `636` is the SSL port used to authenticate with the LDAP Server.
3. When Internet Explorer displays a Security Alert dialog (Internet Explorer 6) or certificate error screens (Internet Explorer 7), click **View Certificate**.

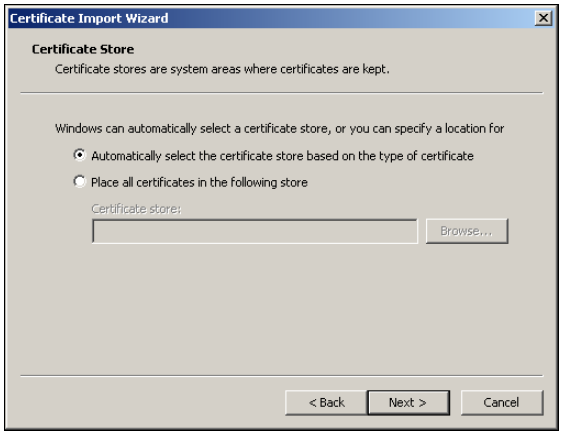
Note Internet Explorer 6 only. All three items in the Security Alert window below must be in compliance. The first item can easily be installed using these instructions; for the middle item, the local CA will need to create a new certificate if it is out of date; for the last item, the name of the certificate will need to match the address entered in the address bar of your browser.

---

4. A Certificate window will open, click on the **Certificate Path** tab.
5. If there is more than on certificate listed in the **Certificate Path** tab, choose the root certificate by selecting the top-most certificate and then clicking **View Certificate**.



6. Choose the **General** tab. and click **Install Certificate**.
7. Click **Next**.


Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
< Back
Next >
Cancel

8. Click **Place all certificates in the following store**.
9. Click **Browse**.

10. Check **Show physical stores** check box.
11. Click the plus sign (+) next to **Trusted Root Certificate Authorities**.
12. Select **Local Computer** and click **OK**.
13. Click **Next** and **Finish** when done.

© 2007 VBrick Systems, Inc.

Resolving Other Security Alerts

If you are receiving any other Security Alerts you will need to identify the problem as either "out of date" or **The name on the security certificate is invalid.** If the certificate has an invalid name, follow the steps below to determine the valid name. If the certificate has an "out of date" error, a new certificate must be created.

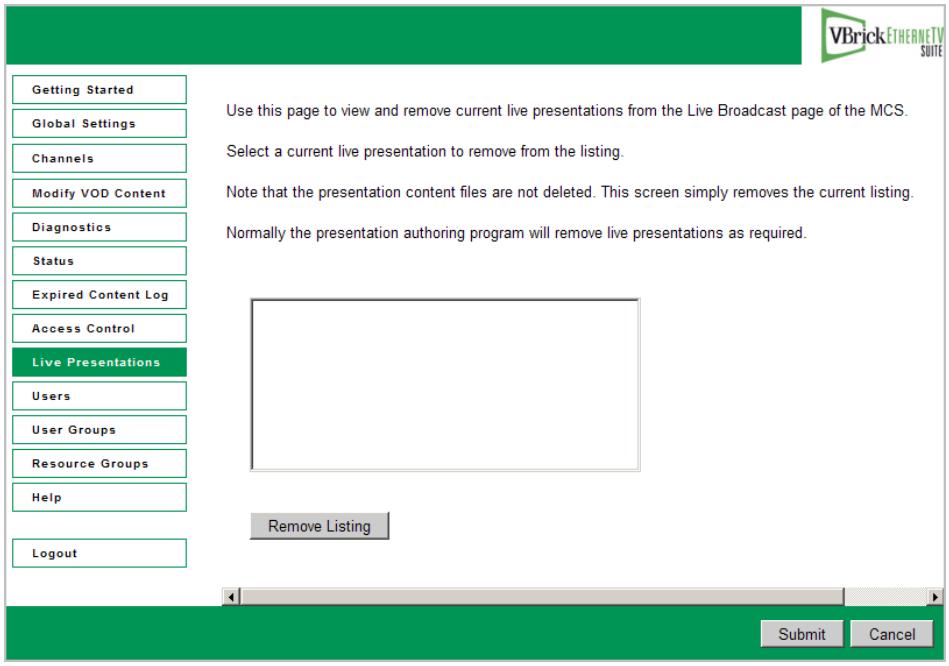
▼ To determine the valid certificate name:

1. Click **View Certificate**.
2. The **General** tab shows who the Certificate is issued to; the address shown is the address that will need to be used in the browser address bar, as well as in the configuration of the LDAP Server.

For example: if the information is `edirldap.vb.loc` then the address bar should read `https://edirldap.vb.loc:636` and the LDAP Path should read `LDAP://edirldap.vb.loc:636` To find out if the address is accessible, ping the address given in a command prompt. If the address is not accessible you must create or add a DNS entry to the Host file on the local server or generate a new certificate with the correct information.

Live Presentations

Use this window to manually remove a live presentation listing from the **Live Broadcasts** page. If the presentation is terminated abnormally for any reason (for example if the presenter exits PowerPoint without going **OFFLINE**), you may need to manually remove the presentation links. See VBPresenter on page 113 for more about configuring live presentations.


Getting Started
Global Settings
Channels
Modify VOD Content
Diagnostics
Status
Expired Content Log
Access Control
Live Presentations
Users
User Groups
Resource Groups
Help
Logout
Use this page to view and remove current live presentations from the Live Broadcast page of the MCS.
Select a current live presentation to remove from the listing.
Note that the presentation content files are not deleted. This screen simply removes the current listing.
Normally the presentation authoring program will remove live presentations as required.
Remove Listing
Submit
Cancel

Users

See Configuring Users on page 91.

User Groups

See Configuring User Groups on page 97.

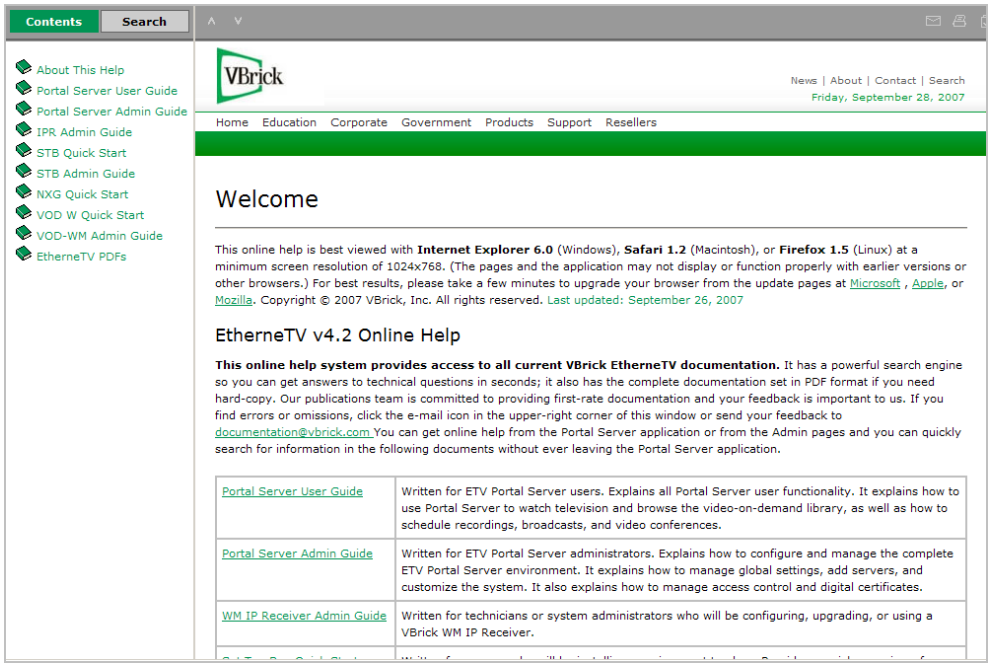
Resource Groups

See Resource Groups on page 99.

Help

This command launches the ETV Portal Server online help system in a new window. This online help system provide fast full-text search and makes it easy to find the information you need. To navigate in the help window, use the tree controls on the left to expand a topic and the navigation buttons at the top to move to a different page. Go to **About this Help > Using this Help** for information about how to Print pages and use the full text Search feature.

© 2007 VBrick Systems, Inc.


Contents
Search
About This Help
Portal Server User Guide
Portal Server Admin Guide
IPR Admin Guide
STB Quick Start
STB Admin Guide
NXG Quick Start
VOD W Quick Start
VOD-WM Admin Guide
EtherneTV PDFs
VBrick
News | About | Contact | Search
Friday, September 28, 2007
Home Education Corporate Government Products Support Resellers
Welcome
This online help is best viewed with Internet Explorer 6.0 (Windows), Safari 1.2 (Macintosh), or Firefox 1.5 (Linux) at a minimum screen resolution of 1024x768. (The pages and the application may not display or function properly with earlier versions or other browsers.) For best results, please take a few minutes to upgrade your browser from the update pages at Microsoft , Apple, or Mozilla. Copyright © 2007 VBrick, Inc. All rights reserved. Last updated: September 26, 2007
EtherneTV v4.2 Online Help
This online help system provides access to all current VBrick EtherneTV documentation. It has a powerful search engine so you can get answers to technical questions in seconds; it also has the complete documentation set in PDF format if you need hard-copy. Our publications team is committed to providing first-rate documentation and your feedback is important to us. If you find errors or omissions, click the e-mail icon in the upper-right corner of this window or send your feedback to documentation@vbrick.com You can get online help from the Portal Server application or from the Admin pages and you can quickly search for information in the following documents without ever leaving the Portal Server application.
Portal Server User Guide
Written for ETV Portal Server users. Explains all Portal Server user functionality. It explains how to use Portal Server to watch television and browse the video-on-demand library, as well as how to schedule recordings, broadcasts, and video conferences.
Portal Server Admin Guide
Written for ETV Portal Server administrators. Explains how to configure and manage the complete ETV Portal Server environment. It explains how to manage global settings, add servers, and customize the system. It also explains how to manage access control and digital certificates.
WM IP Receiver Admin Guide
Written for technicians or system administrators who will be configuring, upgrading, or using a VBrick WM IP Receiver.

Logout

This command logs you out of the application and lets you log back in as a different user. This may be necessary to gain access to certain functionality. For example, some users may not be allowed to create thumbnails and you may want to login as a user who has the permissions to do this.

© 2007 VBrick Systems, Inc.

Chapter 4

Users and User Groups

Topics in this chapter

Overview 87
Configuring Users and User Groups 89
Configuring Users 91
Configuring User Groups 97
Resource Groups 99
STB Authentication 100

Overview

Adding the EtherneTV system to a network provides many benefits in the form of increasing access to rich media. However, because of the sensitive nature of some video assets, many customers want to limit access to different users or groups of users. VBrick's EtherneTV Portal Server allows Administrators to setup the system in just this manner. The ETV Portal Server makes it easy to provide different Users or User Groups access to different resources. The ETV Portal Server Access Control system allows administrators to allow/deny access to the portal server for Windows-based PCs, Macintoshes, and Set Top Boxes:

- Viewing of certain Live Channels
- Viewing of stored content from specific VOD folders
- Publishing content to specific VOD folders
- Recording content to a specific VOD folder
- Allow the viewing of content from only specific VOD servers on the network
- The ability to place bandwidth restrictions for viewing content
- The ability to limit certain users to only access Multicast or RTSP (unicast) content
- The ability to group content resources (Live Channels and/or VOD content) into Resource Groups, which allows the setup and modification of the Access Control functionality to take place much more easily.

The ETV Portal Server is permissive by default, meaning, authentication is not enabled and access to the entire functionality of the server is allowed. However, to follow good security practices, once the Access Control functionality is enabled on the Portal Server, all resources are by default *not* available to any users. Administrators need to provide access to resources to different users or user groups.

Definitions

The ability to provide different users different access to resources on a network is typically referred to as access control, authentication and authorization, and/or access management. VBrick refers to this functionality as Access Control. In order to fully understand the range of functionality of the ETV Portal Server Access Control system, it is beneficial to define some of terms that are used in this section.

Authentication

Authentication is the process of identifying an individual, usually based on a username and password. In security systems, *authentication* is distinct from *authorization* (see below), which is the process of providing individuals access to resources based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

The ETV Portal Server Access Control system allows administrators to authenticate users against the ETV Portal Server database or authenticate users against an LDAP directory. More details on the different authentication databases are given below.

Authorization

Authorization is the process of granting or denying access to a network resource. Most computer security systems are based on a two-step process. The first stage is *authentication*, which ensures that a user is who he or she claims to be. The second stage is *authorization*, which allows the user access to various resources based on the user's identity. In the ETV Portal Server, all authorization is done directly on the ETV Portal Server, through the ETV Portal Server database.

LDAP

LDAP (Lightweight Directory Access Protocol) is a set of protocols for accessing information directories. The LDAP standard defines both a network protocol for accessing information from the directory and an extensible structure for defining how the information is organized in the directory. The advantage of using an LDAP directory is centralized management of users. For example, a new user needs only to be entered once into the LDAP directory and all future modifications to that user can be done in the same central location. Different applications can authenticate and/or authorize users against the LDAP directory.

There are numerous LDAP directory products on the market today, but the most popular are Microsoft Active Directory, Novell eDirectory, Sun iPlanet, and OpenLDAP. *VBrick supports major LDAP vendors but only Microsoft Active Directory and Novell eDirectory are fully tested and supported.*

VBrick Database

The ETV Portal Server server ships by default with the MySQL database, which is a fully ODBC-compliant database. (Open Database Connectivity is a standard database access method.) For those environments that have not migrated to an LDAP directory-based user management system, all of the authentication functionality can be done directly in the ETV Portal Server database itself. Also, for those environments that are using LDAP directories for Authentication, all of the Authorization functionality also takes place in the ETV Portal Server database. Additionally, to reduce the chance of system lockout, all Administrative Users are located in the ETV Portal Server database.

Resources and Resource Groups

In the ETV Portal Server, providing a user with Resources refers to providing them access to a particular functionality of the EtherneTV system. These include the ability to view Live Channels, to view VOD content, to publish content to the VOD, and to record content or schedule a recording. A unique feature of the ETV Portal Server software is the ability to group Resources into Resource Groups. This allows the administrator to quickly and easily assign several resources at once to specific Users or User Groups.

© 2007 VBrick Systems, Inc.

Configuring Users and User Groups

1. Setup and Configure ETV Components

The following products need to be setup and properly configured prior to configuring Access Control.

1. **ETV Portal Server** – The ETV Portal Server needs to be properly setup and configured on the network. The following items should be configured in the Portal Server interface:
   a. If there is a VOD server(s) in the system, the proper addresses for these servers need to be entered into the Portal Server Administrative pages and connectivity to those servers should be ensured.
   b. The folder structure on the VOD server should be defined (even if there is no content in these folders) as folders are how the Access Control functionality provides access to end users to view VOD content, publish content, and record content. When setting up the folder structure, the Administrator should be thinking about how they plan to provide access to different groups of users. For example, if a corporation wanted to provide certain content to the Engineering group and certain content to the Marketing group, then they would want to set up an Engineering folder and a Marketing folder on their VOD server.
   c. If there are live streams on the network, then those streams should be provided a channel number if the Administrator wants to provide access to live streams via channel number.
   d. If security is a concern, SSL should be turned on between clients and the ETV Portal Server server. This allows User Names and Passwords to be encrypted between the client and the server. See the section Configuring for SSL on page 103 for instructions on how to configure this.

2. **VBrick** – If there are VBricks in the network, they are auto-discovered but still need to be added to the Portal Server database.

3. **VOD Server** – If there are VOD servers in the network, again they need to have connectivity to the Portal Server and the folder structure needs to be configured.

4. **Set-Top Boxes** – If there are STBs to be deployed in the system, they should be configured with a Host Name, and should be configured to point to the ETV Portal Server.

Additionally, if an LDAP server is going to be used to authenticate users, then the administrator should know the address of the server, the group structures on the LDAP server, and the Context (if the server is not Microsoft's Active Directory).

Note In order to scan the Groups available in Microsoft's Active Directory, in Windows Explorer, go to **Tools > Folder Options**. On the **General** tab, make sure that the **Show common tasks in folders** is selected. Then go to **Start > My Network Places** and select **Network Tasks > Search Active Directory**.

---

2. Choose an Authentication Method

Select one of the following methods:

VBrick Database	The native ETV Portal Server user database provides local authentication for users and administrators.

LDAP Database	Enables the ETV Portal Server to authenticate against, and retrieve user and group data from, an existing LDAP server.

Both methods can be used simultaneously. If LDAP authentication is enabled, the ETV Portal Server will attempt to authenticate against the LDAP server first, and if this is unsuccessful, will attempt to authenticate against the local ETV Portal Server User Database.

VBrick Database

If authentication is enabled, you must select a database (either VBrick or LDAP). The VBrick (ETV Portal Server) user database contains user, group, and resource information that provides the Portal Server with information to allow it to provide the appropriate privileges to users and Set-Top Boxes that are accessing the system. Administrators should authenticate users with the native Portal Server user database if:

- User authentication is required, but the organization does not have an LDAP server.
- For STBs, the organization wishes to use User PINs. Since User PINs are not available in the LDAP directory, the users need to be created in the ETV Portal Server database (Note: only those users that need PINs to access STBs need to be created in the ETV Portal Server database. PC or Mac users can still be authenticated against LDAP).

LDAP Directory Server

An LDAP directory server contains User and Group information which the ETV Portal Server can authenticate against to verify User's identities. The Portal Server then uses this information to authorize users to access the system. Administrators should authenticate users with an LDAP Directory server if:

- The organization has an LDAP server that they actively manage to allow products to authenticate.
- The ETV Portal Server administrator can obtain the necessary configuration information from the LDAP administrator to allow the authentication to occur.

Using LDAP reduces the amount of administrative time necessary to add and modify users from the ETV Portal Server system. VBrick Systems encourages customers who have LDAP directories implemented to use them for authentication with the ETV Portal Server.

3. Create User Groups on the Portal Server

Grouping users is common practice and makes administering access to the ETV Portal Server less complicated than administering access by individual user. The ETV Portal Server allows the administrator to create groups, specify group memberships for users, and set access privileges for the group. A user can be a member of one group or multiple groups. Group access privileges also can be set and modified on a per group basis.

If an LDAP directory is being used for Authentication, the same group information that is available in the directory can be used to Authorize end users to access the ETV Portal Server. For example, if the organization has three User Groups in its LDAP directory—Marketing, Engineering, and Sales—they can simply create these groups in the ETV Portal Server system, and assign privileges to the groups.

© 2007 VBrick Systems, Inc.

4. Create Resource Groups on the Portal Server

In the Portal Server software, providing a user with Resources refers to providing them access to a particular functionality of the EtherneTV system. These include the ability to:

- View Live Channels.
- View VOD content.
- Publish content to the VOD.
- Record content or schedule a recording.
- Launch an emergency broadcast.

A unique feature of the Portal Server software is the ability to group Resources into Resource Groups. This allows the administrator to quickly and easily assign several resources at once to more than one User or User Groups. This also makes the ongoing management of this content for these Users or User Groups much easier.

For example, if the organization has three User Groups—Marketing, Engineering, and Sales—they might create four resource groups. These Resource Groups would be Full Access, which are resources that everyone can see, and one Resource Group for each of the user groups. Full Access would be assigned to all user groups, and the Marketing Resource Group would be assigned to the Marketing User Group, the Engineering Resource Group to the Engineering User Group, and the Sales Resource Group to the Sales User Group.

Resource Groups provide the added bonus that they allow the Administrator to quickly provide access to new content to Users and User Groups. For example, if the organization originally had ten Live Channels on the network, and another Live Channel was added, the Administrator would simply need to add that Channel to the appropriate Resource Groups and the channel would be available.

5. Create Users on the ETV Portal Server

Creating users is an optional step that can be completed for the following reasons.

- The organization needs to provide a single user with additional privileges above and beyond what is available to his or her User Group or Resource Group.
- The organization wants to authenticate STB users using a PIN.
- Users can be assigned to multiple User Groups.

6. Assign Resources to Users or User Groups

The final step is to provide access to Resources to Users and/or User Groups. The administrator can assign individual resources to Users or User Groups, or can assign Resource Groups (if created) to Users or User Groups. Detailed information on the steps to configure access control and provide access to resources to Users and/or User Groups is provided in the following sections.

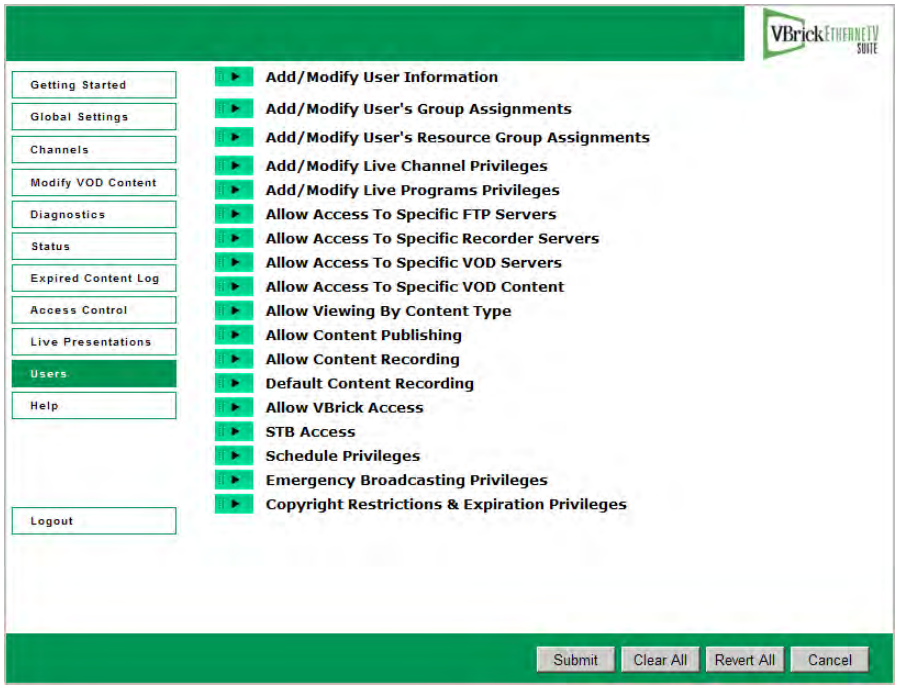
Configuring Users

There are several different ways to provide privileges to different User and User Groups with the ETV Portal Server. The easiest way is to use the group structure of an existing LDAP database. LDAP User Groups can be added to the ETV Portal Server system and assigned permissions (see User Groups below). All of the users in this group will have the same

permissions. For ease of implementation, VBrick recommends configuring User Groups and Resource Groups (see these sections below), prior to configuring users.

However, if further individual permissions need to be assigned, administrators can add them as a user. Under the users section, administrators have the ability to add, modify and delete users. Submit may be pressed at anytime during the process or can be done when everything has been added/modified. Users will have the permissions of the group as well as the additional permission that are assigned to them. The ETV Portal Server is additive in its permissions, meaning that it takes all of the permissions that are provided to a particular user and provides all of these to the user.

Users can be added by using the VBrick Database if LDAP authentication is not available or desired. Finally, in order to assign user PINs to access Set-Top Boxes, a user assignment is needed (see Set-Top Box Authentication section below). Note that STB PIN access is dependent on the VBrick Database being enabled. See Access Control on page 76 for details.



Submit	Save changes and/or navigate to the next window.
Add New	Takes the administrator to the Add New User, User Group, or Resource Group screen (depending on which section you are in)
Clear All	Clears any entries that have been entered in the individual sections.
Revert All	Returns all entries to the last state entered in the database. This selection is important if a mistake is made during entry.
Cancel	Cancels out of the page. Changes are not saved.
Clear	Clear eliminates or de-selects any entries in the particular section.
Revert	Returns the selection to the last state entered in the database. This selection is important if a mistake is made during entry.

© 2007 VBrick Systems, Inc.

Once all selections have been made, you can press **Submit** in the bottom right hand corner of the screen (or any of the other buttons shown above) to submit the information to the database. User privileges include the following options:

Add/Modify User Information 93
Add/Modify User's Group Assignments 94
Add/Modify User's Resource Group Assignments 94
Add/Modify Live Channel Privileges 94
Add/Modify Live Program Privileges 94
Allow Access to Specific FTP Servers 95
Allow Access to Specific Recorder Servers 95
Allow Access to Specific VOD Servers 95
Allow Access to Specific VOD Content 95
Allow Viewing by Content Type 95
Allow Content Publishing 96
Allow Content Recording 96
Default Content Recording 96
Allow VBrick Access 96
STB Access 96
Schedule Privileges 97
Emergency Broadcast Privileges 97
Copyright Restrictions & Expiration Privileges 97

Add/Modify User Information

To add or modify users, select **Users** from the navigation bar on the left.

User	• **User** – Use this option if the EtherneTV system will be accessed by a PC or Mac user, or if Users will be authenticated to STBs via PIN numbers. This access is not limited to a specific PC or STB. • **Set Top Box** – Use this option if the EtherneTV system will be accessed via a STB attached to a television or other video display. If Set-Top Box is selected, then the privilege to the system will be on a per STB basis. The authentication will take place automatically, so no end user interaction is required. When choosing STB, the STB's host name or IP address must be entered, as well as an optional location/description of the STB.
Username	To authenticate using an LDAP database, the user name must match exactly what is in the LDAP database (the Portal Server is case sensitive). A new user can also be assigned (if using the VBrick database option) that does not exist in the LDAP database.
Password	For LDAP authentication a password is not needed (the user will use their normal network login password). If using the VBrick database a password must be entered (passwords are case sensitive).

STB Pin	Optional. A PIN number can be assigned to a user that allows them to access their content from any STB, regardless of the STB's privilege level. This works well when an STB is going to be a shared resource. Note: STB PIN access is dependent on VBrick Database being enabled.
First Name	Optional. User first name.
Last Name	Optional. User last name.
E-mail address	Optional. User e-mail address.
Location	Optional. User location.

Assigning Privileges to Users

There are three ways to assign privileges to users:

- Assign the User to a User Group that has privileges assigned to it.
- Assign the User to a Resource Group that has privileges assigned to it.
- Individually assign resources to the User.

These methods all can be combined. For example, to provide a User with access to the resources provided to a User Group but also provide them access to additional resources, the administrator can a) Assign the User to that Resource Group and b) Individually assign the additional resources to that user. Each of these methods is discussed below.

Add/Modify User's Group Assignments

Users can be assigned to specific User Groups, and they will inherit the privileges of that group. If no User Groups appear, then none have been defined. Click User Groups in the main navigation to the left to create User Groups.

Add/Modify User's Resource Group Assignments

Users can be assigned to specific Resource Groups, and they will inherit the privileges of that Resource Group. If no Resource Groups appear, then none of been defined. Click Resource Groups in the main navigation to the left to create Resource Groups.

Add/Modify Live Channel Privileges

A "live channel" is a live stream that has been modified into a Custom station or a TV station and assigned a channel number. A list of available live channels will be displayed. A user can be provided access to all live channels or to individual live channels.

For live channels, both the Channel Number and the Station Name will appear in the Channel Guide. If the Channel number is selected, the ETV Portal Server will always provide access to the particular channel (for example, Channel 1) even if the Program Name of that channel changes. If the Station Name is selected, the ETV Portal Server will always provide access to the station (for example, CNN), even if the channel that it is associated with changes (for example, from Channel 2 to Channel 4).

© 2007 VBrick Systems, Inc.

Note The live streams shown in the Portal Server may also be restricted by a bit mask on a VBrick encoder. The Portal Server will parse the bitmask and send the live stream only to ETV clients with a IP address that matches the masked IP of the source VBrick. You can use this feature in addition to the Portal Server authorization features. See the Announce(SAP) parameter in the *MPEG-2*, *MPEG-4*, or *WM Appliance Admin Guide* for more information.

Add/Modify Live Program Privileges

"Live programs" are all live streams that are available. These are unmodified, unassociated streams. Use this option to restrict access to specific live streams.

Allow Access to Specific FTP Servers

Allow or deny access to defined FTP servers.

Allow Access to Specific Recorder Servers

Allow or deny access to defined recorder servers.

Allow Access to Specific VOD Servers

Choose from a list of available VOD server(s) to which a user has access. A user can have access to multiple servers. This feature is particularly useful when VOD servers are located in different physical locations that are separated by low bandwidth links. For example, if a company has offices and VOD servers in both New York and Chicago, and these offices are separated by a T-1 link, then they would want to limit the users in the Chicago office to the Chicago VOD server and those in New York to the New York VOD server.

Note When a user is provided access to particular VOD server(s), and they are given the privilege to Publish or Record to a particular folder, when they Publish or Record, the video will be Published or Recorded to each server that they have access to. This is important for clustering purposes.

Allow Access to Specific VOD Content

Choose from a list of folders to which a user can have access. A user can have access to multiple folders on multiple servers. If the user has access to multiple VOD servers, and the folder names are the same on both servers, only one folder name will show up in the list.

Allow Viewing by Content Type

The Administrator can limit the types of content that a user can view and/or limit the bandwidth that specific users can view. Note that this setting does not apply to URLs that were manually added by an administrator (see URLs on page 52).

Do Not Allow Multicast viewing	This will limit users that are on a non-multicast capable part of the network from trying to view multicast video.
Restrict Multicast to Kbps	This will limit users to only viewing multicast streams that are a certain size or smaller. This works well to maintain bandwidth utilization over a particular WAN port.

Do Not Allow RTSP viewing	This will limit users from viewing RTSP Unicast Streams from MPEG-4 Encoders and from accessing RTSP unicast streams from a Video-on-Demand server (MPEG-1, MPEG-2, or MPEG-4). This works well to maintain bandwidth utilization over a particular LAN or WAN port.
Restrict RSTP viewing to Kbps	This will limit users to only viewing RTSP streams that are a certain size or smaller. This works well to maintain bandwidth utilization over a particular LAN or WAN port.

Allow Content Publishing

Administrators can allow a user the ability to publish content to folder(s) on an VOD Video-On-Demand Server. This function allows the user access to the **Add Video** page, where users can add pre-recorded video content to a VOD. It also allows users to (1) create (and upload) **Thumbnails** for video files in the folders to which they can publish, to (2) delete video content from the VOD server, and (3) to add keyword and description data using the **Modify Info** button. To prevent users from deleting content, be sure this option is disabled.

Note If users are provided access to more than one VOD server, when they publish content, it will be published to each of the servers to which they have access. This is important for clustering purposes.

Allow Content Recording

Used for scheduled recording. Administrators can allow a user the ability to schedule the recording of live content to a specific folder(s) on a VOD Video-On-Demand Server. They cannot record content to any other folder(s). You must select a folder here to enable **Default Content Recording** below. If there is no schedule license, **Allow Content Recording** is not shown as an option and **Default Content Recording** lets you select any folder. If you add a schedule license later (using **Start > Control Panel > Add or Remove Programs)**, **Allow Content Recording** will be shown as an option with all folders selected. You may want to unselect specific folders in order to restrict recording privileges.

Default Content Recording

Used for on-demand recording. You must select a folder above for **Allow Content Recording** before you can make a folder selection here. Administrators can allow a user the ability to record live content to a specific default folder on an VOD Server by pressing the **Record** push button below the Preview Window. For ease of use, the Administrator can only assign one default folder where a particular user can record content. This allows one button recording on the ETV Portal Server and is particularly important for Set-Top Box users, who may not be able to enter a recording path with their IR remote control.

Allow VBrick Access

Administrators can allow a user the ability to access all VBricks or only specific VBricks when scheduling events. When scheduling an event, users will see only those VBricks for which they have been granted access.

© 2007 VBrick Systems, Inc.

STB Access

Administrators can allow a user the ability to access all STBs or only specific STBs when scheduling events. When scheduling an event, users will see only those STBs for which they have been granted access.

Schedule Privileges

Users may have full, partial, or no permission to schedule VBrick event. Users with full privileges can modify all configuration parameters in a schedule. Users with partial privileges *cannot* modify **Advanced Settings**.

- Super – can change all schedules.
- Full – can change only "owned" schedules.
- Partial – can change only "owned" schedules; no **Advanced** features.
- None – cannot create schedules; no **Add** button shown on Scheduling page.

Emergency Broadcast Privileges

Administrators can specify whether or not a user can launch Emergency Broadcasts.

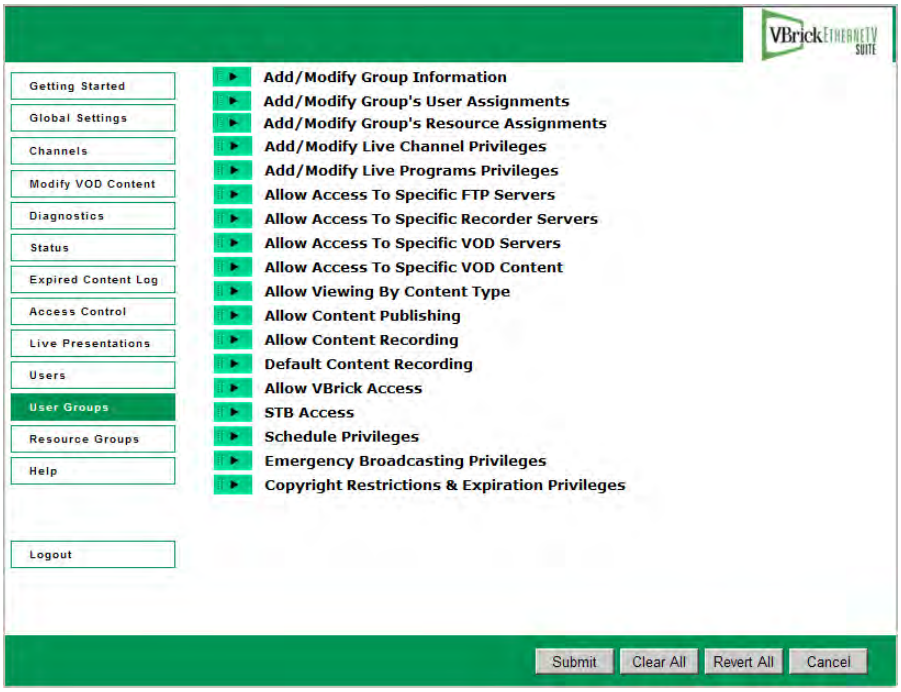
Copyright Restrictions & Expiration Privileges

Administrators can allow users to set Copyright Restrictions and Expiration Privileges when adding stored content or scheduling a recording. Note that copyright restrictions apply only to Portal Server-initiated playback sessions (and not, for example to direct RTSP requests to a VOD server).

Configuring User Groups

Grouping users is common practice and makes administering access to the ETV Portal Server less complicated than administering access by individual user. The ETV Portal Server server allows the administrator to create User Groups, specify group memberships for users, and set access privileges for the group. A user can be a member of one group or multiple groups. Group access privileges also can be set and modified on a per group basis.

If an LDAP directory is being used for Authentication, the same group information that is available in the directory can be used to Authorize end users to access the ETV Portal Server. For example, if the organization has three User Groups in its LDAP directory—Marketing, Engineering, and Sales—they can simply create these groups in the ETV Portal Server system, and assign privileges to the groups.



Add/Modify Group Information

If LDAP is being used for authentication, then the group name has to exactly match the group name in the LDAP directory. If LDAP is not being used, Group Names can be entered directly into the ETV Portal Server database. If Microsoft's Active Directory is used, to find the available list of active groups in **Windows XP**, browse to **My Network Places** and click on the left-hand menu **Search Active Directory**. A new window will open. Click **Find now** to see all available groups. In **Windows 2000**, go to **My Network Places > Entire Network > Directory**, the domain, and **Users**.

Note Windows XP needs to be configured to **Show Common Tasks in Folders**. To configure this, in **My Network Places**, go to **Tools > Folder Options**. In the **General > Tasks** section, select the radio button called **Show common tasks in folders**.

Add/Modify Group's User Assignments

Users can be assigned to specific User Groups, and they will inherit the privileges of that group. If no Users appear, then none have been defined. However, if LDAP is being used for Authentication, no users need to be defined. When a user Authenticates to the system, the Authentication process will return the User's group information. The user will receive the privileges that are provided to that group.

Add/Modify Group's Resource Assignments

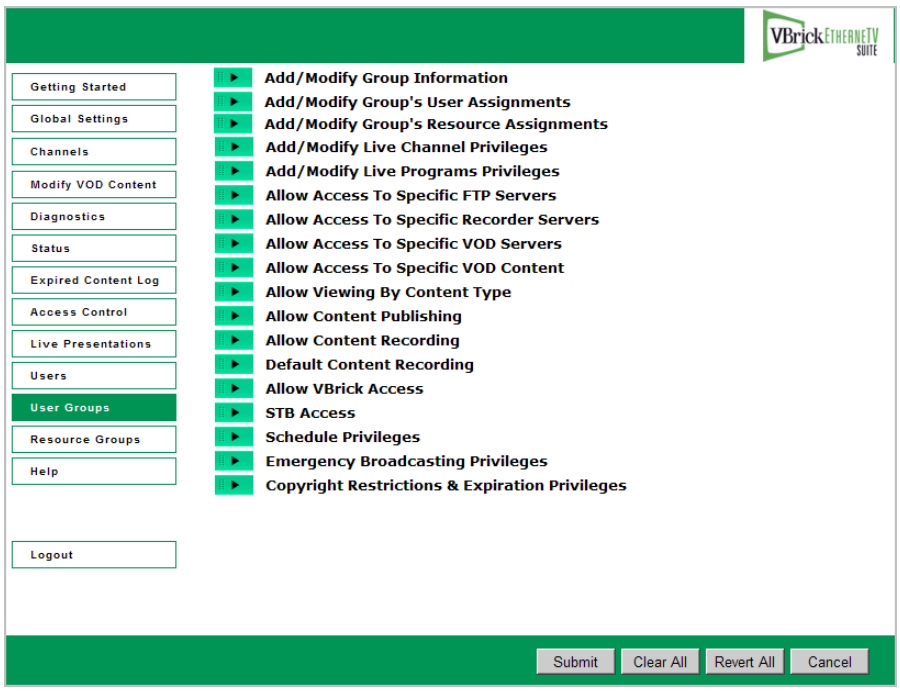
Resource groups can be assigned to User Groups, and the User Group will inherit the privileges of that Resource Group. If no Resource Groups appear, then none of been defined. Click **Resource Groups** in the main navigation to the left to create Resource Groups.

© 2007 VBrick Systems, Inc.

Note The remaining options for **User Groups** (beginning with **Add/Modify Live Channel Privileges**) are the same as those described earlier for individual Configuring Users on page 91. The only difference is that the descriptions will apply to groups of users rather than to individual users.

Resource Groups

In the ETV Portal Server software, providing a user with Resources refers to providing them access to a particular functionality of the EtherneTV system. These include the ability to view Live Channels, to view VOD content, to publish content to the VOD, and to record content. A unique feature of the ETV Portal Server software is the ability to group Resources into Resource Groups. This allows the administrator to quickly and easily assign several resources at once to more than one User or User Groups. This also makes the ongoing management of this content for these Users or User Groups much easier.



For example, if the organization has three User Groups—Marketing, Engineering, and Sales—they might create four resource groups. These Resource Groups would be Full Access, which are resources that everyone can see, and one Resource Group for each of the user groups. Full Access would be assigned to each user group, and the Marketing Resource Group would be assigned to the Marketing User Group, the Engineering Resource Group to the Engineering User Group, and the Sales Resource Group to the Sales User Group. Resource Groups provide the added bonus that they allow the Administrator to quickly provide access to new content to Users and User Groups. For example, if the organization originally had ten Live Channels on the network, and another Live Channel was added, the Administrator would simply need to add that Channel to the appropriate Resource Groups and the channel would be available.

Add/Modify Resource Group Information

Add the Resource Group Name that is relevant for the Resource Group being created.

Add/Modify User's Resource Assignments

Users can be assigned to specific Resource Groups, and they will inherit the privileges of that Resource Group. If no Users appear, then none have been defined. Click on the Users section to add Users.

Add/Modify Group's Resource Assignments

User Groups can be assigned to Resource Groups, and the User Group will inherit the privileges of that Resource Group. If no User Groups appear, then none have been defined. Click User Groups in the main navigation to the left to create User Groups.

Note The remaining options for **Resource Groups** (beginning with **Add/Modify Live Channel Privileges**) are the same as those described earlier for individual Configuring Users on page 91. The only difference is that the descriptions will apply to resource groups rather than to individual users.

STB Authentication

There are two ways (STB IP address or user PIN) to authenticate and authorize Set-Top Boxes in the ETV Portal Server. STB access control is slightly different from PC and Macintosh-based authentication (which uses the commonly employed User Name and Password mechanism). The two methods are outlined in the table below.

Table 12. Authentication Methods

Method	Description	User Interaction	Comment
User PIN	If Access Control is enabled, but the STB is not defined in the system, then Access Control works based on a user PIN. This PIN is defined on a *per user* (not per STB) basis, so that users need to be defined for this to work.	When the user logs into the system, they will be prompted for their PIN. The user simply enters the PIN with the remote control or the wireless keyboard, and can then access the video.	This implementation is appropriate for environments where multiple users with different privileges will be accessing the same STB. An example of this would be a shared classroom where multiple teachers are accessing the STB at different times.
STB IP Address or Host Name	The ETV Portal Server system determines the content that the STB can view based on its IP Address or Host Name.	No user interaction is required. The user simply turns on the STB and only the content that the STB user can view id displayed.	This implementation is similar to a cable TV setup, e.g. if the cable plan does not include CNN, that channel cannot be viewed. This implementation is easiest for end users because you do not have to remember user names or PINs. It is appropriate for environments where one or a few people with the same privileges access the same STB.

Authentication by PIN

When an end user accesses the ETV Portal Server via a STB, the Portal Server takes the following steps to authorize users.

© 2007 VBrick Systems, Inc.

1. It determines if there is Authentication/Authorization information associated with the Host Name of the STB. If so, based on the STB Host Name, the ETV Portal Server will present the STB with the information appropriate to its privileges. Note that the ETV Portal Server uses the least restrictive settings when providing access to the system.
2. If there is no Authentication/Authorization information associated with the Host Name of the STB, the user will be prompted for a PIN. A PIN is a user-based mechanism to log onto the STB. When the user enters his or her PIN, the ETV Portal Server authenticates the user against the Portal Server database.
3. Once the user is authenticated, the ETV Portal Server will check the User Groups and/or Resource Groups that the User is associated with and the privileges associated with those groups.
4. After checking the Groups privileges, the ETV Portal Server will check for any individual user privileges above the group privileges.
5. The user will be presented with the information appropriate to their privileges. Note that the ETV Portal Server uses the least restrictive settings when providing access to the system.

If Authentication and Authorization is enabled, but the STB is not defined in the system, then Access Management works based on a User PIN. This PIN is defined on a **per user** (not per STB) basis, so Users need to be setup in the system for this to work. When the user accesses the ETV Portal Server through the STB, they will be prompted for their PIN. The user simply enters the PIN with the remote control or the wireless keyboard, and can then access the video for which they have privilege. This implementation is appropriate for environments where multiple users with different privileges will be accessing the same STB. An example of this would be a shared classroom, where multiple teachers are accessing the STB at different times.

Authentication by Host Name or IP Address

The ETV Portal Server determines the content that the STB can view based on its IP Address or Host Name. No user interaction is required. The user simply turns on the STB, and only the content that the STB user can view displays. This implementation is similar to a Cable Television setup—for example, if the plan does not include HBO, then that channel cannot be viewed. This implementation is easiest from the end user perspective because end users do not have to remember user names or PINs. This implementation is appropriate for environments where multiple people can access the same STB.

The following steps provide best practices for properly configuring the Access Control section of the ETV Portal Server.

© 2007 VBrick Systems, Inc.

Chapter 5

Configuring for SSL

Overview

Secure Sockets Layer (SSL) provides endpoint authentication and communications privacy over the Internet using cryptography. Whenever there is a concern regarding confidentially and integrity of *management* data being sent between ETV Portal Server and external clients, the ETV Portal Server user login page and all admin pages should be configured with a digital X.509 certificate to enable SSL encryption. When SSL encryption is enabled, the Portal Server only encrypts the Login pages and/or the Admin pages. *The actual video streams are never encrypted.* When SSL is enabled, the following elements can be encrypted:

- MCS Admin Console – All MCS Admin Console pages are encrypted to protect management information and other sensitive data.
- MCS User Portal – Only the Login page (including the user ID and password) are encrypted. The video streams are not encrypted.
- LDAP Server – If using LDAP authentication, communications between the Portal Server and the LDAP Server can be encrypted by enabling encryption on the LDAP server.

By convention, URLs that require an SSL connection start with `https` instead of `http`. The steps briefly listed here, and explained in detail on the following pages, explain how to set up and use SSL on the Portal Server.

▼ To set up SSL for client access to the ETV Portal Server:

1. Generate a Certificate Request.
2. Submit a Certificate Request.
3. Install the Certificate on the ETV Portal Server.
4. Configure ETV Resources for SSL.

1. Generate a Certificate Request

If your company does not have a X.509 certificate, or does not have a one for the ETV Portal Server, a new certificate request must first be created.

▼ To generate a certificate request:

1. From the ETV Portal Server, start the Microsoft Internet Information Services (IIS) Manager.
2. Expand the server name and select the web site for which the certificate will be installed.
3. Right-click the web site, and then click **Properties**.
4. Select the **Directory Security** tab.
5. Select the **Server Certificate** button within **Secure** communications to launch the Web Server Certificate Wizard.
6. Select **Next** on the Welcome dialog box.

7. Select **Create a New Certificate** and then select **Next**. (If **Create a New Certificate** is unavailable, the certificate has probably been installed already. If that is the case, skip the rest of the steps, and go to Step 4. Configure ETV Resources for SSL. If you want to create new certificate for ETV Portal Server, select **Remove the current certificate** to remove the certificate first, and then restart the procedure.)
8. Select **Prepare the request now, but send it later** and then select **Next**.
9. Type a descriptive name for the certificate in the **Name** field, type a bit length for the key in the **Bit length** field, and then select **Next**.
10. Type an organization name (e.g. VBrick) in the **Organization** field and type an organizational unit (such as Sales Department) in the **Organizational unit** field, and select **Next**. (This information will be placed in the certificate request, so make sure it is accurate. The Certificate Authority will verify this information and will place it in the certificate. A user browsing the ETV Portal Server will want to see this information in order to decide if they should accept the certificate.)
11. In the **Common name** field, type a common name, and then select **Next**. (**Important:** The common name is one of the most significant pieces of information that ends up in the certificate.)
12. Enter the appropriate information in the **Country/Region**, **State/Province**, and **City/locality** fields, and then select **Next**.
13. Enter a file name for the certificate request. The file contains information similar to the following:

```
------BEGIN NEW CERTIFICATE REQUEST ------
MIIDZjCCAs……
------END NEW CERTIFICATE REQUEST ---------
This is a Base 64 encoded representation of the certificate request. The
request contains the information entered into the wizard and also your public
key and information signed with your private key.
```

14. Select **Next**. The wizard displays a summary of the information contained in the certificate request.
15. Select **Next** and select **Finish** to complete the request process.

2. Submit a Certificate Request

If a CA-signed Certificate from a trusted Certificate Authority (such as VeriSign or Thawte) is going to be purchased, the certificate can now be sent to a CA for verification and processing. After the certificate response is received from the CA, the installation process can continue on the ETV Portal Server. Purchasing a CA-signed certificate will cause a security alert in the browser upon access to the server.

3. Install the Certificate

▼ To install the certificate on the ETV Portal Server:

1. Start the Microsoft Internet Information Service (IIS) Manager.
2. Expand the server name and select the web site for which the certificate will be installed.
3. Right-click the web site and then select **Properties**.
4. Select the **Directory Security** tab
5. Select **Server Certificate** to launch the Web Server Certificate Wizard
6. Select **Process the pending request and install the certificate** and then click **Next**.

© 2007 VBrick Systems, Inc.

7. Enter the path and file name of the file that contains the response from the CA, and then click **Next**.
8. Examine the certificate overview, click **Next**, and then click **Finish**. A certificate is now installed on the ETV Portal Server.

4. Configure ETV Resources for SSL

After installing the certificate on the ETV Portal Server, the ETV Portal Server can now be configured for SSL. This is a two-step process (1) first you configure the Portal Server user login page for SSL access, and (2) configure the Portal Server Admin pages for secure SSL access. This means that when a user attempts to access the Portal Server user pages it will automatically bring them to `https://<ipaddressofserver>` for the user pages. Users will notice a padlock icon at the bottom of their screen while logging into the Portal Server, however the padlock will disappear once they login. When an administrator attempts to access the Administration pages it will also force them to use `https://<ipaddressofserver>/admin`. The padlock icon will be visible at the throughout the entire Admin site.

Securing the Portal Server User Pages

▼ To configure the ETV Portal Server User Pages for SSL access:

1. Go the Portal Server install location, typically `C:\Program Files\VBrick\MCS` and open `web.config` in a text editor.
2. Uncomment the sections labeled Web Page Security 1, 2, and 3 **by deleting only the <!-- and --> characters shown below in red.**

Web Page Security 1

```
<!-- Web Page Security 1: Remove comments around the following section to enable
SSL on the login page. -->
<!--
<section name="secureWebPages"
type="Hyper.Web.Security.SecureWebPageSectionHandler, WebPageSecurity"
allowLocation="false" />
-->
```

Web Page Security 2

```
<!-- Web Page Security 2: Remove comments around the following section to enable
SSL on the login page. -->
<!--
<secureWebPages mode="On" maintainPath="False" warningBypassMode="AlwaysBypass"
bypassQueryParamName="BypassSecurityWarning">
<file path="login.aspx" /> <file path="login4.aspx" /> </secureWebPages>
-->
```

Web Page Security 3

```
<!-- Web Page Security 3: Remove comments around the following section to enable
SSL on the login page. -->
<!--
<add name="SecureWebPage" type="Hyper.Web.Security.SecureWebPageModule,
WebPageSecurity" />
-->
```

Securing the Portal Server Admin Pages

▼ To configure the ETV Portal Server Admin pages for SSL access:

1. Go the Admin Console location, typically `C:\Program Files\VBrick\MCS\Common\MCS Admin Console` and open `web.config` in a text editor.

2. Uncomment the sections labeled `Web Page Security 1` and `Web Page Security 2` **by deleting only the <!-- and --> characters shown below in red.**

Web Security 1

```
<!-- Web Page Security 1: Remove comments around the following section to enable
SSL on all Admin Console pages. -->
<!--
<section name="secureWebPages"
type="Hyper.Web.Security.SecureWebPageSectionHandler, WebPageSecurity"
allowLocation="false" />
-->
```

Web Security 2

```
<!-- Web Page Security 2: Remove comments around the following section to enable
SSL on all Admin Console pages. -->
<!--
<secureWebPages mode="On" maintainPath="False" warningBypassMode="AlwaysBypass"
bypassQueryParamName="BypassSecurityWarning">
<directory path="/" recurse="True" />
</secureWebPages>
-->
```


© 2007 VBrick Systems, Inc.

Chapter 6

Network Video Recording

Topics in this chapter

NVR Overview 107
NVR Types. 109
NVR Installation 110
NVR Configuration 110
Using an NVR 111

NVR Overview

The Network Video Recorder (NVR) provides a dedicated platform to perform multiple simultaneous recordings of live streams coming from VBrick encoders. The NVR lets you off-load all recording tasks from the ETV Portal Server machine to one or more separate "recorder server" machines. The NVR provides the ability to record live streams from the network, store these recorded video files on a specified location (a record server or other network location), and optionally automatically transfer the contents to selected locations, and/or ingest them to VOD servers.

The NVR is available in two versions—one that supports 10 simultaneous records and one that supports 40—and is ideal for environments that require large scale recording on a robust and reliable platform. The NVR is tightly integrated with the Portal Server, the Scheduler, and VBrick's Video-on-Demand servers. The NVR provides these standard features.

- Dedicated platform – NVR servers are available on a dedicated hardware platform which eliminates resource contention and guarantees successful recording.
- Software only – NVR servers are available as a software-only option which you can install on your own server hardware. See the *NVR Release Notes* for server hardware recommendations.
- Redundant storage – both NVR servers offer RAID 5 for storage redundancy as well as dual power supplies.
- Large storage capacity – the NVR 10 provides 720 GB of storage; the NVR 40 provides 1492 GB.
- Load Balancing – Load balancing is used when multiple NVR servers are installed. Rather than recording to a specified server, the system records to a dynamically selected server based on a load balancing algorithm.
- Software Development Kit – VBrick provides an SDK to interface with the Portal Server or the NVR. In a typical security, surveillance, and monitoring applications application (without a complete Portal Server), you can write a custom application that will record streams directly to a standalone NVR.

In a basic Portal Server installation (without an NVR), the standard recording functionality allows a maximum of two concurrent recordings. In order to expand this recording capability, you can purchase a Network Video Recorder to offload recording tasks and improve overall

performance. The Portal Server and/or the NVRs are delivered with all software installed or as a software-only option. The NVR comes in standard and standalone versions as explained below. The only difference is in functionality. *Both record either 10 or 40 concurrent streams depending on the license you purchase*. Both versions can be expanded to include multiple, additional NVRs so that your recording capacity is virtually unlimited.

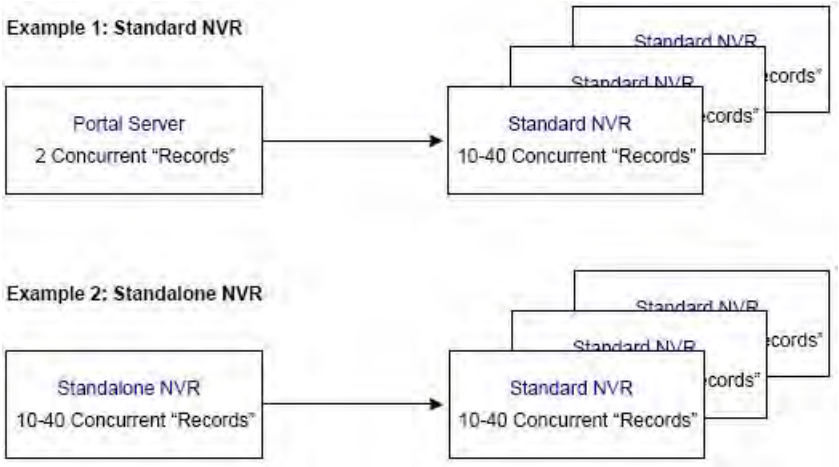


Figure 12. Standard and Standalone NVR Examples

NVR Hardware

The NVR is comprised of both hardware and software. If you purchased the hardware/software combination from VBrick, each platform (standard or standalone) comes fully loaded with NVR software. The following table shows the hardware configuration relative to the number of purchased licenses. The license file determines the total maximum concurrent recordings allowed. *In a standard NVR installation the NVR license file is stored on the Portal Server; in a standalone NVR installation the NVR license file is stored on the Standalone NVR.*

Table 13. NVR Hardware Specifications

	NVR – 10 Record Licenses	**NVR – 40 Record Licenses**
Platform	Dell PowerEdge 2950	Dell PowerEdge 2950
Simultaneous records	10	40
Storage capacity	(2) 73 GB OS drives (4) 146 GB content drives	(2) 146 GB OS drives (4) 300 GB content drives
RAID Type	2 drive RAID1 for OS drives 4 drive RAID5 for content drives	2 drive RAID1 for OS drives 4 drive RAID5 for content drives
CPU	(1) 3 GHz dual core	(2) 3 GHz dual core
RAM	1 GB DDR RAM	2 GB DDR RAM
Chassis	2U	2U
Power supply	Redundant	Redundant
Operating System	Windows Server 2003 Web Edition or Standard Edition	Windows Server 2003 Web Edition or Standard Edition

© 2007 VBrick Systems, Inc.

NVR Performance Considerations

The NVR 40 lets you record any combination of up to 40 MPEG-1, MPEG-2, MPEG-4, and WM streams at a time. There are however performance considerations when recording multiple, simultaneous, high-rate MPEG-2 or WM streams. At MPEG-2 rates up to 5.5Mbps or WM rates up to 1.2Mbps 40 simultaneous recordings are supported. At higher rates however the full licensing capacity cannot be used. For example, when using the **Best Quality** WM template at 4.5Mbps, 10 simultaneous records are supported; when using MPEG-2 at 15Mbps, 15 simultaneous recordings are supported.

NVR Types

Standard NVR

A Standard NVR's record capability is managed by a Portal Server or Standalone NVR. In a standard NVR installation, the full Portal Server or Standalone NVR application is installed on one machine and the NVR application is installed on a separate machine. If you need to add recording capacity, you can add multiple NVRs as necessary. You use the Portal Server or a Standalone NVR application to configure the Standard NVR (see Configuring a Standard NVR). A *standard* NVR has these characteristics:

- supports record only.
- records 10 or 40 concurrent streams depending on license.
- is configured with the standard Portal Server Admin Console *or* the Standalone NVR Console.
- records from the **Record** button *or* the **Scheduler** module.
- Supports "batch" recording where one large file is recorded into multiple smaller files.

Note When purchasing additional NVRs, VBrick provides a single combined license that includes recording capacity for all NVRs onsite.

Standalone NVR

A Standalone NVR manages the record capability of itself and any attached Standard NVRs. *A standalone NVR is typically used in security, surveillance, and monitoring applications or anywhere where full Portal Server functionality is not required.* In a standalone NVR installation, a subset of the Portal Server application is installed on one machine and the NVR application is installed on the same machine *or on a different machine*. If you need to add recording capacity, you can add multiple Standard NVRs necessary. You use the subset of the Portal Server application to configure the NVR (see Configuring a Standalone NVR). A *standalone* NVR has these characteristics:

- supports record only.
- records 10 or 40 concurrent streams depending on license.
- is configured with a subset of the Portal Server Admin Console that has limited features—no VBricks, STBs, etc.
- records from the **Scheduler** module only.
- has limited end user features. End users can see only the **Scheduler**, the **Status** page, and the **Help** system.
- supports "batch" recording where one large file is recorded into multiple smaller files.

- has an API interface that lets you write custom applications to control the NVR.

Note When purchasing additional NVRs, VBrick provides a single combined license that includes recording capacity for all NVRs onsite (Standard and/or Standalone).

NVR Installation

See the NVR Release Notes for complete installation instructions.

Synchronizing the Portal Server and the NVR

The internal clocks on the Portal Server and the NVR must be synchronized for recording functionality to work properly. You can use the `Net time` command as explained below or you can use an external time server. In order to run the `Net time` command on *either* server, the server must be on the domain, and the user logged onto the server must have admin privileges *and* be part of the domain.

▼ To synchronize the Portal Server and the NVR:

1. Open a command prompt window on the Windows 2003 Server *Portal Server* machine.
2. Type: **`Net time \\{NVR IP Address} /SET`**

NVR Configuration

Configuring a Standard NVR

A standard NVR is installed on a dedicated machine that comes fully loaded with all NVR software. However, you must still configure the NVR as explained below. NVR configuration is performed using the Recorders pages on the Portal Server's or Standalone NVR's Admin Console. See Recorders on page 43 for more information.

▼ To configure a standard NVR in a *Portal Server Installation*:

1. Login to the Portal Server Admin Console using *the host name or IP address of the Portal Server machine*. For example: `http://myserveraddress/admin`
2. Define a Record server.
   a. Set record **Path** if necessary. Set to local hard drive on NVR or to a network drive.
   b. Set **Max. Recording**.
3. Define VOD and FTP Servers (go to **Global Settings > Servers**).
   a. Record only – VOD server not required.
   b. Record and ingest – must define a VOD server.
   c. Record, ingest, and FTP – must define VOD and FTP servers.
   d. Record and FTP – must define an FTP server.
4. If Access Control is enabled, you must create a user and grant the following permissions on the **Users** page in the Admin Console. See Configuring Users on page 91 for more information.
   a. **Add/Modify Live Channel Privileges**
   b. **Allow Access To Specific FTP Servers**
   c. **Allow Access To Specific Recorder Servers**
   d. **Allow Access To Specific VOD Servers**

 © 2007 VBrick Systems, Inc.

e. **Allow Content Recording**

f. **Schedule Privileges**

Configuring a Standalone NVR

▼ To configure a standard NVR in a *Standalone NVR Installation*:

1. Login to the Standalone NVR Admin Console *using the host name or IP address of the Standalone NVR machine*. For example: http://myserveraddress/admin
2. Define a Record server.
   a. Set record **Path** if necessary. Set to local hard drive on NVR or to a network drive.
   b. Set **Max. Recording**.
3. Define VOD and FTP Servers (go to **Global Settings > Servers**).
   a. Record only – VOD server not required.
   b. Record and ingest – must define a VOD server.
   c. Record, ingest, and FTP – must define VOD and FTP servers.
   d. Record and FTP – must define an FTP server.
4. If Access Control is enabled, you must create a user and grant the following permissions on the **Users** page in the Admin Console. See Users on page 81 for more information.
   a. **Allow Access To Specific FTP Servers**
   b. **Allow Access To Specific Recorder Servers**
   c. **Allow Access To Specific VOD Servers**
   d. **Allow Content Recording**
   e. **Schedule Privileges**

Using an NVR

As noted, the Portal Server and the Network Video Recorder are installed on separate machines. Using the Admin Console, you configure the NVR by indicating where record files will be stored, and defining the maximum number of simultaneous recording the NVR will support (which is less than or equal to the licensed number of recordings). The record **Path** can be set to local hard drive on the NVR machine or to a network drive. In a Portal Server installation, from PCs or STBs, end users can access NVR record features (record start/ record stop) through using the Portal Server. When a recording is initiated using the **Record** button on the **Live Broadcasts** page of the Portal Server, the record file is be automatically ingested to available VOD servers, based on the stream type (e.g. MPEG2, MPEG4, etc.) and user's permissions. After ingestion, the record file can be automatically deleted from record server based on the Global Settings configuration.

When a record is initiated through Scheduler interface of Portal Server, end users can specify whether they want to FTP the recorded file to available FTP servers or to ingest the recorded file to available VOD servers. They can also specify whether or not to automatically delete the file after a successful FTP or ingestion. (These options are not available in "batch" mode. If you select **Enable Batch**, the files are not FTPed and ingested; they are saved to D:\Inetpub\ftproot\MCS\Record and all other options are disabled.)

In a *standard* NVR configuration, live streams can be recorded (1) by using the **Record** button on the embedded player or (2) by using the **Scheduler** module. In a *standalone* NVR installation, recording can *only* be initiated from the **Scheduler** module using the interface as

shown below in Figure 13. For a complete description of the Scheduler, see "Using the Scheduler" in the *Portal Server User Guide*.

Note To use a standard NVR, the Portal Server and the NVR must be installed and running. To use a standalone NVR, only the NVR application must be running.

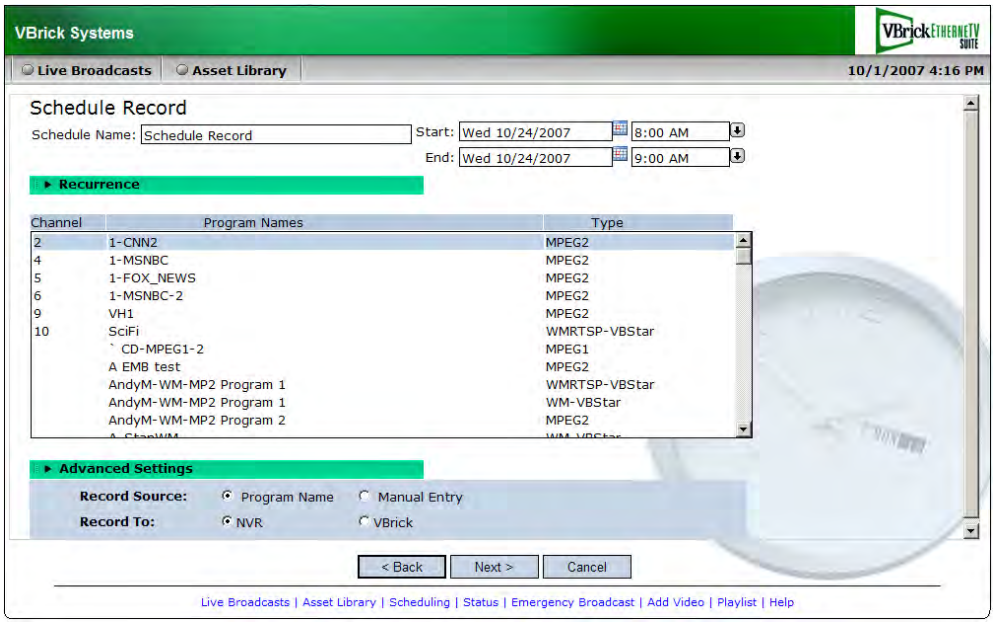


Figure 13. Portal Server "Schedule Record" Page

© 2007 VBrick Systems, Inc.

Chapter 7

VBPresenter

Topics in this chapter

Overview 113
Configuring MCS for VBPresenter 114

Overview

Rich media presentations include those with audio, video, graphics, animation and other multimedia features like synchronized PowerPoint slides. The Portal Server can display live and stored rich media presentations created by VBrick's VBPresenter Powerpoint Add-In. VBPresenter presentations run in Internet Explorer only. Live VBPresenter presentations like the one shown in Figure 14 are available for viewing from the **Live Broadcasts** page; stored presentation are available from the **Video Library** page (and have a special icon). Like other content, rich media presentations can only be seen by those viewers who have appropriate permissions. This document explains how to configure the Portal Server to work with VBPresenter. The *VBPresenter User Guide* explains in detail how to configure and use VBPresenter.

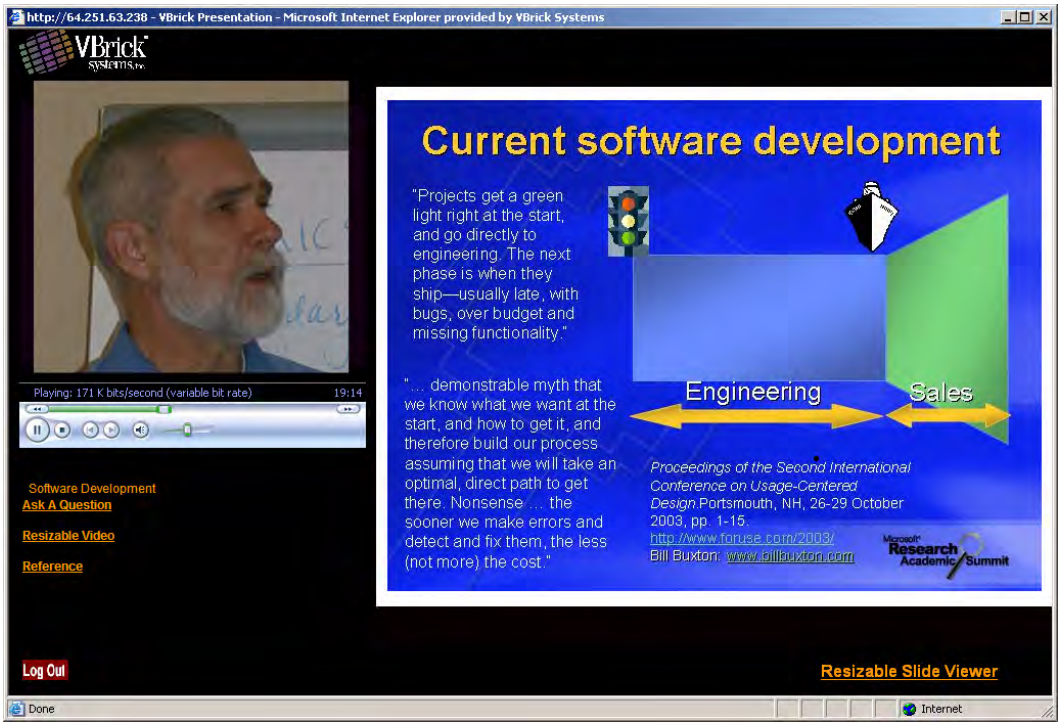

http://64.251.63.238 - VBrick Presentation - Microsoft Internet Explorer provided by VBrick Systems
VBrick systems
Playing: 171 K bits/second (variable bit rate) 19:14
Software Development
Ask A Question
Resizable Video
Reference
Log Out
Current software development
"Projects get a green light right at the start, and go directly to engineering. The next phase is when they ship—usually late, with bugs, over budget and missing functionality."
"... demonstrable myth that we know what we want at the start, and how to get it, and therefore build our process assuming that we will take an optimal, direct path to get there. Nonsense ... the sooner we make errors and detect and fix them, the less (not more) the cost."
Engineering
Sales
Proceedings of the Second International Conference on Usage-Centered Design.Portsmouth, NH, 26-29 October 2003, pp. 1-15.
http://www.foruse.com/2003/
Bill Buxton: www.billbuxton.com
Research Academic Summit
Resizable Slide Viewer
Done
Internet

Figure 14. VBPresenter Rich Media Presentation

Working with Presentations

If you will be working with VBPresenter presentations, be aware that they have the following unique characteristics and limitations.

- They launch in a new browser window in their native user interface—not in the Portal Server.
- They can only be uploaded from VBPresenter—they cannot be added directly or autoingested to the Portal Server.
- They do not work with the Portal Server Scheduler and cannot be scheduled to play in advance.
- They can be recorded for future use only in VBPresenter—they cannot be recorded using the Portal Server.

Configuring MCS for VBPresenter

The following pages explain how to configure the MCS Portal Server to handle live and stored presentations. Once these steps are done, you use the native functionality in VBPresenter to make live or stored presentations available on the Portal Server. For more about configuring and using VBPresenter, see the *VBPresenter User Guide*.

Configuring an FTP User

The Portal Server's **FTP User Name** and **FTP User Password** must be set in the Admin console (**Global Settings > Global Assignments**) to the values that are configured in IIS. When a client logs on to the Portal Server's FTP account (for example from a Command Prompt window), this combination of FTP user name and password must place the user into the FTP root directory of the Portal Server. (This is *not* the same as the Presentations directory. The Presentations directory is a virtual directory in IIS. This directory is the root folder for live presentations only.) There is an MCS directory at the FTP root directory. Note that the entries made in the Admin console are stored in the Portal Server and do not actually configure IIS. These values must reflect what IIS has been configured for.

Configuring a Presentation User

Perform the following configuration *one time only* so that the presentation tool you are using can access the Portal Server. These steps will create a pseudo VBPresenter user who is associated with the authoring tool and has specific permissions on the Portal Server.

▼ To create a presentation user:

1. Open the Admin Console and go to **Users**.
2. Add a user name (for example PresentationUser) and give this user the following permissions:
   a. **Add/Modify Live Channel Privileges** – check the appropriate channels.
   b. **Add/Modify Live Programs Privileges** – check the appropriate programs.
   a. **Allow Access to Specific VOD Servers** – check the appropriate servers.
   b. **Allow Access to Specific VOD Content** – check the appropriate folders.
   c. **Allow Content Publishing** – check the appropriate folders.
3. Go to **Global Settings > Global Assignments > Assign Presentations** and select the user you created above (for example PresentationUser) as the **New Presentation User**.

© 2007 VBrick Systems, Inc.

Configuring for Live Presentations

You must perform the following steps to configure the Portal Server for *each* live presentation.

▼ To configure the Portal Server for a live presentation:

1. Go to **Global Settings > Program Names** and add a program name (for example Live Presentation). Then use this same name in the **MCS Program Name** field in VBPresenter. This is the title that will be displayed on the **Live Broadcasts** page during a live presentation.
2. If necessary, give your end users access to this live presentation. Go to **Users > Add/ Modify Live Channel Privileges** and select this **Program Name**.

Hint To pre-configure a presentation, create a **Program Name** in advance on the Portal Server and assign **Live Channel Privileges** to users. Then use the same name in the **MCS Program Name** field in VBPresenter when giving the presentation. The **MCS Program Name** will be available on the **Live Broadcasts** page for any users who have permissions to view that channel

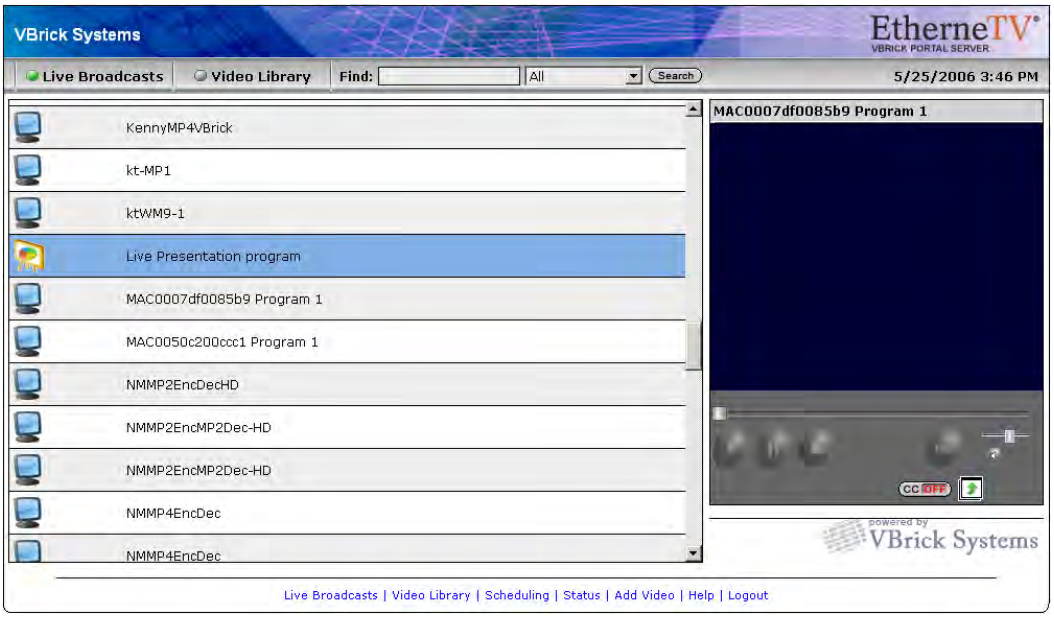
---

Launching a Live Presentation

The web server in VBPresenter can be configured with either a domain name or an IP address. If configured with an IP address, you must launch the MCS client using the IP address in order to view presentations successfully; if configured with a domain name, you must launch the MCS client using the domain name. You cannot mix-and-match domain names and IP addresses or Session Expired and Maximum Viewers Exceeded errors may be displayed by the Portal Server.

▼ To launch a live presentation:

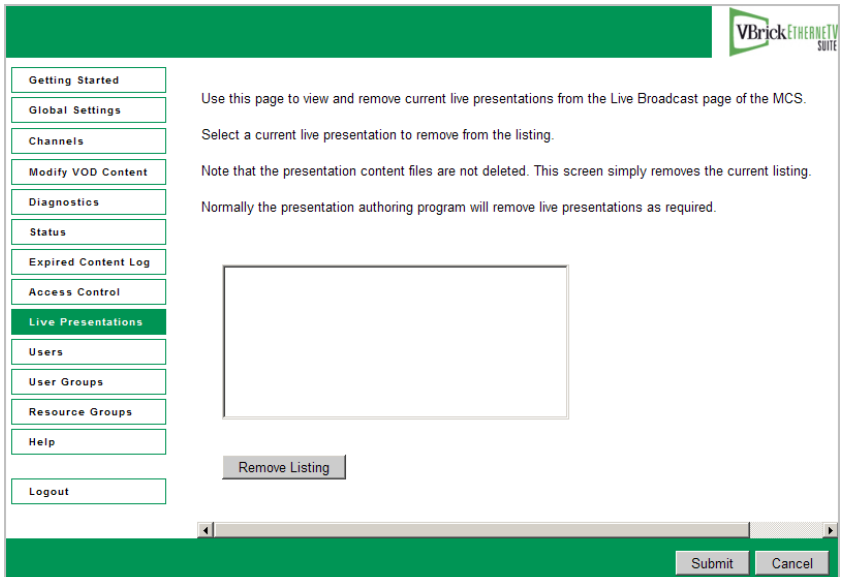
1. Once the Portal Server is configured as explained above, go to VBPresenter, upload your slides, go **LIVE ONLINE**, and begin the presentation. This makes the presentation immediately available to authorized users from a link on the **Live Broadcasts** page in the Portal Server. The link will be automatically removed from this page at the end of the presentation. If the presentation is terminated abnormally for any reason (for example if the presenter exits without going **OFFLINE**), you may need to manually remove the presentation link from the **Live Broadcasts** page. See Live Presentations on page 83 for details.



2. If you also want to record the presentation from VBPresenter, click **Record Start** to begin and **Record Stop** to end.
3. When finished recording, click **Publish Recorded Presentation** on the VBPresenter toolbar. This will FTP the recorded presentation to the Portal Server (with a unique name) and make it available to authorized users on the **Video Library** page. This may take a few minutes.

Removing a Live Presentation

Use this window to manually remove a live presentation listing from the **Live Broadcasts** page. If the presentation is terminated abnormally for any reason (for example if the presenter exits PowerPoint without going **OFFLINE**), you may need to manually remove the presentation links.



© 2007 VBrick Systems, Inc.

Launching a Stored Presentation

▼ To launch a stored presentation:

1. Open the Portal Server user interface.
2. On the **Video Library** page, navigate to the video name published from VBPresenter and click once to launch it in a browser.
3. Mouse over the presentation name to display the **Info** button to the right. Use this popup window to enter **Keyword** and **Description** "metadata" that will make the presentation easy to find in a search.

Configuring for Stored Presentations

There is no additional configuration for stored presentations.

© 2007 VBrick Systems, Inc.

Chapter 8

Auto Content Ingestion

Topics in this chapter

AutoIngest Content 119
AutoIngest Content via XML 121
Removing MPEG-4 Closed Captions 124

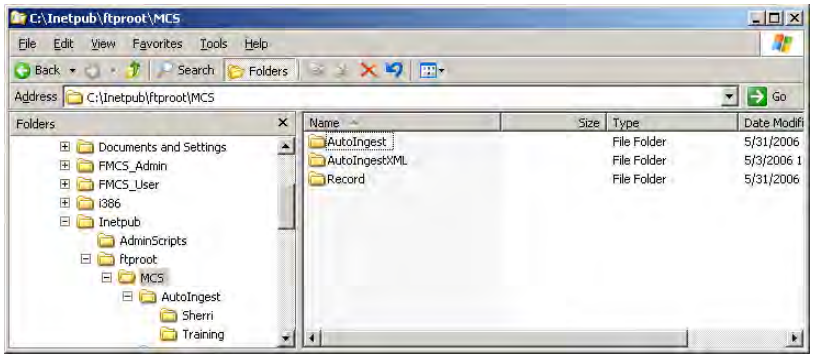
As explained in this chapter, there are two ways to autoingest content depending on your requirements. One method is to FTP or copy your video content to predefined folders on the Portal Server. The folders are monitored and the content is automatically ingested (autoingested) at periodic intervals. The second method is to use .xml files for content stored at remote locations or on mass storage devices. This method also supports metadata for search, copyright protection, maximum viewers, etc.

AutoIngest Content

You can FTP or copy prerecorded content to the ETV Portal Server for easy ingestion to the VOD server(s). The ETV Portal Server periodically (every 5 minutes) polls certain folders for presence of content and if found ingests the content onto multiple VOD servers. This process is called *Automatic Content Ingestion* or *Autoingestion*. The content can come from a pushbutton recording on the Portal Server, a VBrick VBStar, or a file recorded with StreamPlayer Plus.

Note You cannot autoingest VBPresenter or other third-party presentations into the Portal Server. You must use the native FTP facilities in each application.

The content should be placed in a pre-defined sub-folder (`mcs\autoingest`) under the FTP root folder. This pre-defined folder is called the *autoingest root folder*. For example, if the FTP root is at `c:\inetpub\ftproot`, the content could be placed anywhere under `c:\inetpub\ftproot\MCS\AutoIngest`. In this example the `autoingest` root is `c:\inetpub\ftproot\MCS\AutoIngest`.



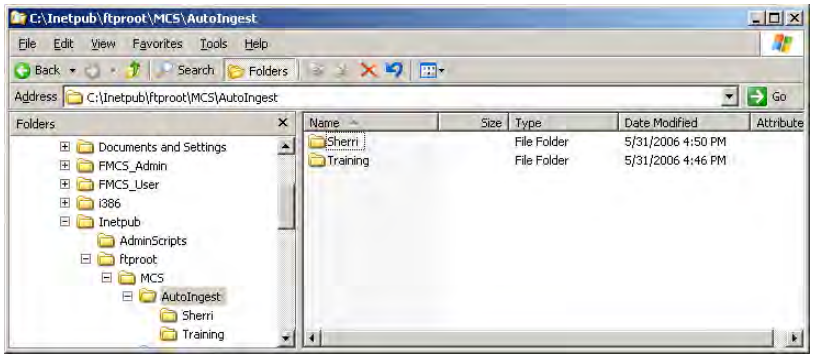
Note The default FTP path may be on a different drive, refer to the IIS default FTP configuration to confirm.

Content that is placed under the autoingest root folder on the ETV Portal Server will be ingested into the root video folder on the VOD server provided that it is configured using the ETV Portal Server Administrator interface. If you want to place content on a subfolder in the VOD server, that same folder would have to be created and configured using the ETV Portal Server Admin interface as described below.

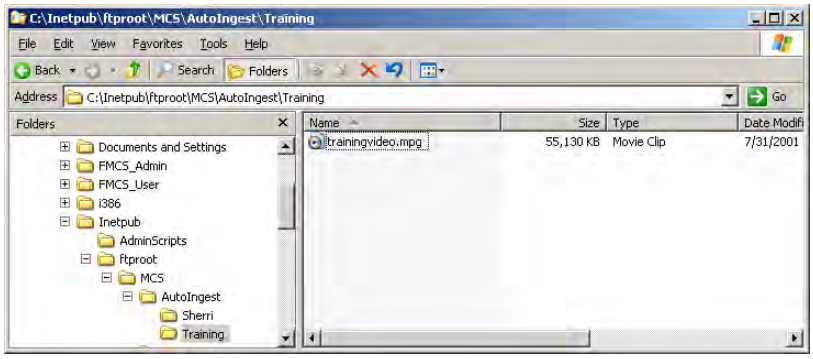
Go to **Global Settings > Servers > Add/Modify Video On-Demand Content Folders**. Here an existing or new folder can be associated with selected VOD servers for autoingestion. The folders are listed on the left with the path relative to autoingest root. The VOD servers are listed on the right inside the **Add/Modify Folders on Selected Servers** box. Select the desired folder and then select the target VOD servers to ingest content. Press **Submit**. The folder is now created under the autoingest root folder and configured. See Add/Modify Video On Demand Content Folders on page 34 for details.

Example

If under the root video folder on the VOD Server you had a folder (or want to create a folder) called `Training` and you wanted `trainingvideo.mpg` to be placed there.

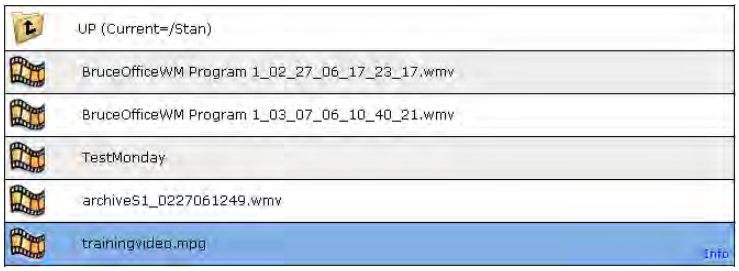


FTP the file to the Portal Server into `<drive:>\inetpub\ftproot\mcs\autoingest\training\`



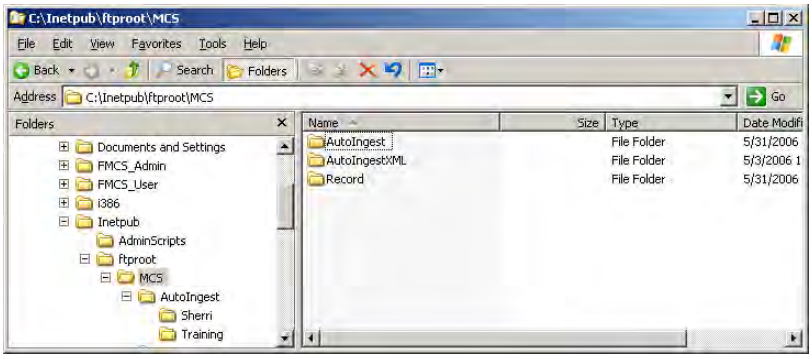
The ETV Portal Server will then ingest the file automatically into the folder on the VOD server(s) that this folder is associated with. The file `trainingvideo.mpg` would be displayed on the ETV Portal Server user interface in the Training folder.

© 2007 VBrick Systems, Inc.



AutoIngest Content via XML

This feature lets you autoingest video files by placing an .xml file in the AutoIngestXML folder on the Portal Server. It also lets you associate metadata with the video such as maximum number of viewers for copyright protection, keywords for searching, etc. As explained below there are three ways (see Table 14) to use this feature depending on where the source files are located. The Portal Server monitors this folder for .xml command files and autoingests any files at five-minute intervals. The ingest command, target video file name, target VOD folder, and metadata to associate with the video are contained in the .xml file. Autoingest permissions are associated with an autoingest user that is defined using the Admin Console.



The Portal Server autoingest folder is under FTP root on the Portal Server at /MCS/AutoIngestXML The video file and the .xml file must be FTPed (or copied) to this directory and the target video title must contain the fully qualified path to the destination. The autoingest user name as configured in the Portal Server Admin Console will be used to access available VOD servers. If the autoingest user does not have publishing rights for the VOD directory specified in the MCSTitle, the ingestion will fail.

Autoingest users must have VOD server access to at least one server capable of storing the video type (WM, MPEG, etc.). Only existing custom fields will be recognized and associated with the video (see Custom Fields on page 25 for more information). The Windows **Event Viewer** will log the ingest command, noting the full path and the .xml data contained in the command, and will also log the successful ingestion of the video.

▼ To create an autoingest user with publishing rights:

1. Open the Admin Console, go to **Users > Add User**, and create an autoingest user, e.g. AutoIngestUser.
2. On the same page, go to **Allow Access to Specific VOD Servers** and select the servers this user can access.
3. On the same page, go to **Allow Content Publishing** and select the folders this user can publish to.

4. Then go to **Global Settings > Global Assignments > Assign AutoIngest** and set the user you just defined as the **Current AutoIngest User**.

AutoIngestXML Modes

There are three modes of operation as shown in Table 14. The mode you use depends on *where* the source files are located.

Table 14. AutoIngest Modes

Mode	Description
Direct	The target source video file is FTPed to the AutoIngestXML folder. The video file and the .xml file must both be FTPed to this folder. In Direct mode, you must FTP the video file first or the ingestion will fail.
Absolute	WM files only. The target source video file resides in a folder on the Portal Server. Only the .xml file is FTPed to the AutoIngestXML folder. This is useful for mass storage devices because you do not have to copy the files to the AutoIngestXML folder on the Portal Server.
Remote FTP †	MPEG Files only. The target source video file resides on a remote FTP server. Only the .xml file is FTPed to the AutoIngestXML folder.

† Not available for VOD-D (Darwin) servers. Use Direct mode only to AutoIngest to VOD-D servers.

Using the XML Template

There are three named templates in the VBrick\MCS\utils folder for Direct, Absolute, and Remote FTP files. Use the appropriate template to manually create an .xml file for *each* video file. Use Notepad, TextPad, or a similar tool and then FTP this file (and the video in Direct mode) to the AutoIngestXML folder on the Portal Server. (In Direct mode, you must FTP the video file first or the ingestion will fail.) The filename can be any alphanumeric string with an .xml extension. The following code shows a sample .xml file that uses the Direct mode template. **The template for each mode is the same except for the SourceFileName and SourceFileType tags**. Table 15 explains the required format for these tags.

```
<?xml version="1.0" encoding="utf-8"?>
<AutoIngestCmd version="1.0">
  <Command>ingest</Command>
  <Ingest>
    <MCSTitle>/VODFolder/Spiderman Returns</MCSTitle>
    <Keywords>Ingest001</Keywords>
    <Description>My ingested Video</Description>
    <Expiration>20060430-1130</Expiration>
    <SourceFileName>Ingest002.wmv</SourceFileName>
    <SourceFileType>WM</SourceFileType>
    <MaxViewers>-1</MaxViewers>
    <FileLink filename="myfile.ppt" url="http://www.google.com/" />
    <FileLink filename="myother.ppt" url="http://www.google.com/" />
    <CustomFields>
        <Field name="CustomTextField1" value="Value1" />
        <Field name="CustomTextField2" value="Value2" />
        <Field name="CustomDropField1" value="one" />
        <Field name="CustomDropField2" value="two" />
    </CustomFields>
  </Ingest>
```


© 2007 VBrick Systems, Inc.

```
</AutoIngestCmd>
```

Table 15. AutoIngestXML Tags

Tag	Description
Command	Required. Must be set to `ingest`.
MCSTitle	Required. Cannot be blank. Must begin with "/" and contains fully qualified path to destination VOD folder/title on the Portal Server. The autoingest user name must have publishing rights for VOD target folder.
Keywords	Optional. Keywords associated with this video. Used for search.
Description	Optional. Description of the video. Used for search.
Expiration	Optional. Content expiration specifier, e.g. `20060430-1130`. Format: `yyyymmdd-hhmm` Used for copyright protection.
SourceFileName	Required. Contains the source video file name to be ingested. The format of this data determines the mode of operation. • Direct – All files. This file must reside in the `AutoIngestXML` directory (*it must be FTPed first*) on the Portal Server. This file will ultimately be copied to one or more VOD servers. The format is simply the filename for example: `ingest001.wmv` • Absolute – WM files only. This file must reside in a folder on the Portal Server. The format for this data is: `[absolutepath] <FullLocPath>` for example `[absolutepath]c:/Temp/ingest002.wmv` • Remote FTP – MPEG Files only. This file resides on a remote FTP server. The format for this data is: `ftp://username:password@FTPServerURL/VirtuualDirectory/Filename` For example: `ftp://videos:videos@172.22.2.1/videos/ingest0003.mpg` where the FTP protocol string, username, password, FTP URL, virtual directory, and file name are specified in the string in a fixed format.
SourceFileType	Format type of the video files: WM, MPEG-1, MPEG-2, MPEG-4. Required for Absolute and FTP Remote modes; not used with Direct.
MaxViewers	Optional. Maximum number of concurrent viewers allowed. -1 = unlimited. If unspecified, -1 (unlimited) is assumed.
FileLink	Optional. 0–n file reference links to associate with this video. Each file link requires a filename (e.g. `"myfile.ppt"`) and a URL.
CustomFields	Optional. 0–n custom fields to associate with this video. See Custom Fields on page 25 for more information. Each custom field must contain: • name – must be already defined in Portal Server or field will be ignored. • value – dropdown list boxes only; must be already defined in Portal Server or field will be ignored.

Removing MPEG-4 Closed Captions

MPEG-4 files with closed captions cannot be added to the EtherneTV-VOD Video-on-Demand server until the closed caption track is removed. The ETV Portal Server will display an error message if you try to add such files. VBrick provides a utility to remove the closed captions track from an MPEG-4 file if necessary. It is installed with ETV Portal Server in `c:\program files\vbrick\utils`

▼ To remove the closed captions track from MPEG-4 files:

1. Go to `c:\program files\vbrick\utils` and double-click `CCTrackRemover.exe`
2. Enter an **MPEG-4 File Name** and click **Remove CC Track**. Depending on the size of the file it may take a few moments to complete.
3. When done, you can add or autoingest the video file as necessary.

© 2007 VBrick Systems, Inc.

Chapter 9

Database Backup

Introduction

The EtherneTV Portal Server uses MySQL to manage the database of users and groups, and also the video *information* related to content on the VOD Servers. Note that this procedure backs up information in the MySQL database only. *It does not back up any video content you may have stored on attached VOD servers.* (To back up video content, you will likely need a backup strategy and a robust storage capability.) Use this procedure when removing the VOD server for troubleshooting purposes, or when upgrading the software, in order to avoid the loss of this content information. Use the backup procedure described here to ensure that data loss is minimal when you restore the database after a transfer or removal of VOD servers. This procedure can also be helpful for load balancing and failover. It can simplify the task of maintaining multiple servers with the same information.

Note In order to backup database files, you will need administrative access to the ETV Portal Server and a safe location to store the backup database and files.

Database Backup

To ensure a successful database backup, you must follow the exact sequence of steps shown below. Also, since this process will interrupt any streaming video, you may want to schedule this procedure at night or during non-business hours.

▼ To back up the database:

1. Log into the Portal Server as the Administrator.
2. The MySQL Service will need to be stopped in order to have a clean copy of the database. Go to **Start > Control Panel > Administrative Tools > Services**.
3. Right-click on **MySQL** in the right pane and select **Stop**. There will be a list of other services that will stop. Take note of these other services and select **Yes**.
4. The Service Control window will show the progress of the Services being stopped. After the services have stopped minimize the Services window.
5. Open **My Computer** and save copies of the following directories in a safe backup location.

```
C:\Program Files\MySQL\MySQL Server x.x\data
C:\Program Files\VBrick\MCS\Logs
C:\Program Files\VBrick\MCS\Images\Thumbnails
C:\Program Files\VBrick\MCS\MCSPresentations
C:\Program Files\VBrick\MCS\Presentations
C:\Program Files\VBrick\MCS\StationIcons
C:\Program Files\VBrick\MCS\licenses
```

6. To restart the **Services**, maximize the **Services** window.
7. Right-click on the **VBrick Object Starter** and select **Start**. This will start the **MySQL** services. If the EtherneTV Scheduler Module or other services were stopped in Step 3 above they will need to be started as well.

Database Restore

To ensure a successful database restore, it is critical that you follow the exact sequence of steps shown below. Also, since this process will interrupt any streaming video, you may want to schedule this procedure at night or during non-business hours.

Note The database cannot be restored from a different version number of ETV Portal Server or from the same version number after additional features (e.g. ETV Scheduler) have been installed. To ensure a successful restore, always perform a backup after an upgrade or after installing new features. Restore the database only to an ETV Portal Server instance with the same version number and with the same features installed.

▼ To restore the database:

1. Log into the Portal Server as the Administrator.
2. The MySQL Service will need to be stopped in order to have a clean recovery of the database. Go to **Start > Control Panel > Administrative Tools > Services**.
3. Right-click on **MySQL** in the right pane and select **Stop**. There will be a list of other services that will stop. Take note of these other services and select **Yes**.
4. A Service Control window will show the progress of the Services that will be stopped. After the services have stopped, minimize the **Services** window.
5. Open **My Computer** and recover the following directories from the backup location.

```
C:\Program Files\MySQL\MySQL Server x.x\data
C:\Program Files\VBrick\MCS\Images\Thumbnails
C:\Program Files\VBrick\MCS\licenses
```

6. To start the Services, maximize the **Services** window.
7. Right-click on the **VBrick Object Starter** and select **Start**. This will start the **MySQL** services. If the EtherneTV Scheduler Module or other services were stopped in Step 3 above they will need to be started as well.

© 2007 VBrick Systems, Inc.

Chapter 10

Amino Set Top Box

Topics in this chapter

Overview 127
Connecting the Amino 127
Configuring the Amino 128
Configuring the Remote Control for a TV 130
Configuring the Amino for a Widescreen 130

Overview

The AmiNet110 is a compact set top box for the Portal Server manufactured by Amino Systems. It connects to a standard TV and plays MPEG-2 streams only—no other streams are selectable for viewing or adding. These pages explain how to connect and configure the Amino set top box. There is no software installation required: simply connect and configure the device as explained below and you are done. The *Portal Server User Guide* explains how to use the Amino remote control unit to select streams and navigate Portal Server pages *after* the Amino is configured and running as explained here. The Amino *does not* support the following Portal Server functionality:

- Access Logging
- Scheduling
- Custom Fields
- Device Control
- Emergency Broadcast
- Copyright Restrictions

Connecting the Amino

Connect the Amino STB to a standard TV and to your Ethernet network as explained below. If necessary, refer to the illustrations in the *AmiNet110 User Guide* that came with the device. Check the components for damage as you unpack the device. The AmiNet110 includes a power supply, a mounting stand, a remote control, and an A/V cable.

▼ To setup and connect the Amino:

1. Mount the Amino either vertically or horizontally as explained in the *AmiNet110 User Guide*.
2. Connect the Amino to your network using a standard Ethernet cable (not supplied) with an RJ-45 connector.
3. Connect the Amino to the TV as follows.

a. Connect one end of the Amino A/V lead to the composite connector on the Amino.
b. Connect the other end to either the S-Video connector on the TV or to the red, white, and yellow audio and video connectors.

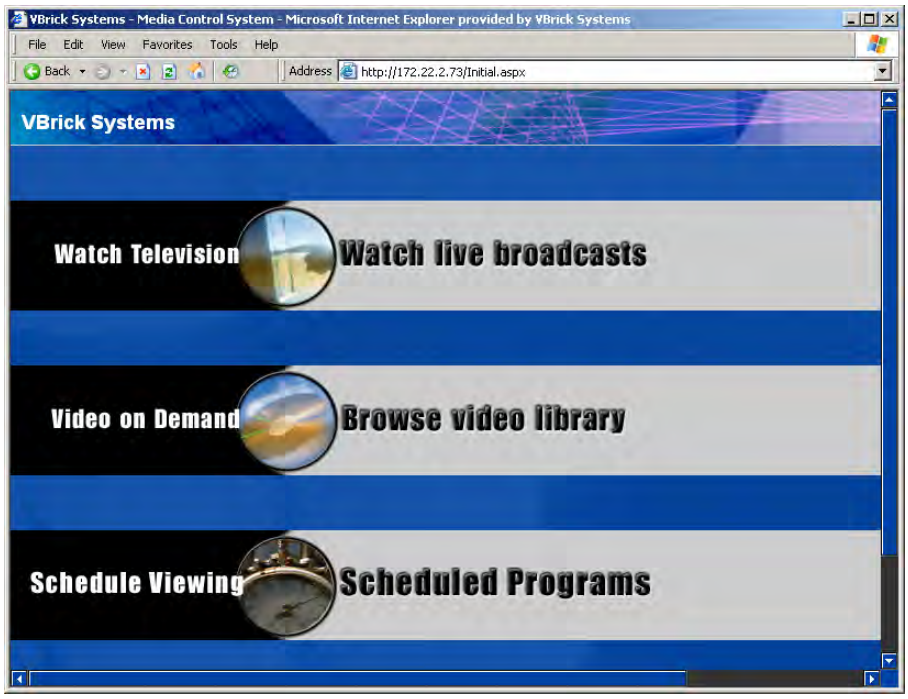
4. Connect the power supply and install three AAA batteries in the remote control.

Configuring the Amino

The Amino STB is shipped with a handheld IR remote control and an optional wireless keyboard. **You must use the Amino wireless keyboard to configure the set top box**.

▼ To configure the Amino using the wireless keyboard:

1. Connect the Amino, the network, and the TV as explained above and power on the STB.
2. When the Amino splash page is displayed, press **Alt-m** on the keyboard.
3. Enter the read management password (default = **leaves**).
4. If a DHCP server is present, the Amino IP address is automatically obtained from the DHCP server.
5. If a DHCP server is not present, and you want to set a static IP address, select **Network Configuration**, set **DHCP Info** to **Do not use**, and enter the new IP address and other network data.
6. Select **Trusted Domains** and add the Portal Server IP address or host name to the list of trusted domains in the format: <**ip_address**> or <**hostname**> (do not use http://). Also verify that **Macrovision** and **JavaScript** are enabled.
7. Save changes and enter the write management password (default = **snake**).
8. Return to main menu and select **Browser Setup**.
9. In the **Home Page** field, enter the Portal Server URL as **http://<PortalServerIPaddress>**
10. Save your changes and push the **Home** button on the keyboard to launch the Amino MCS home page (Figure 15).



© 2007 VBrick Systems, Inc.

Figure 15. Amino MCS Home Page

11. Click on **Watch live broadcasts**, for example, to display the Live Broadcasts page (Figure 16). You can use this page to select any available MPEG-2 stream.

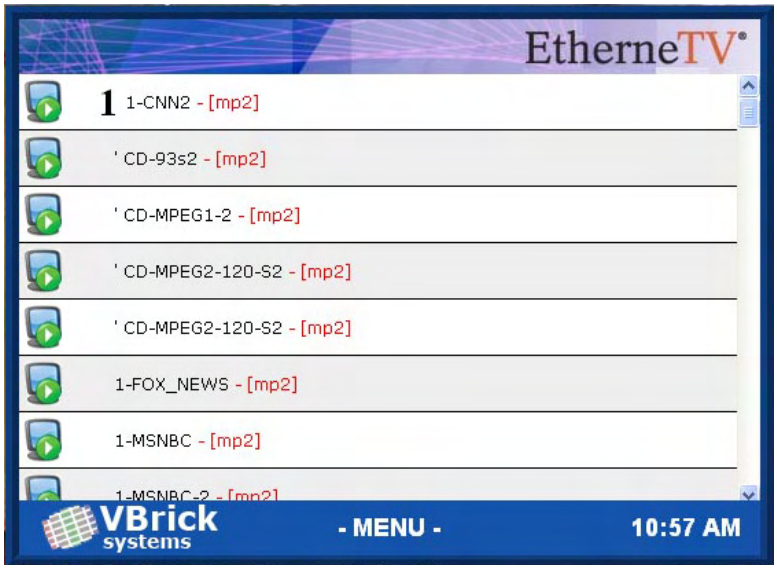


Figure 16. Live Broadcasts Page

Changing the IP Address

Once the Amino is initially configured as explained above, you can change the IP address as necessary using the wireless keyboard.

▼ To change the IP address:

1. Go to the Amino MCS home page (Figure 15) and press **Ctrl** on the keyboard.
2. Click **OK** to toggle the **Default Amino Keys** to **On**.
3. Press **Alt-m** on the keyboard and use the steps listed above in Configuring the Amino to set a new IP address.
4. Press **Ctrl** again to toggle off the **Default Amino Keys** and resume normal operation.

Configuring a Direct Connection

In some cases you may wish to connect the Amino directly to a VBrick MPEG-2 appliance without using the Portal Server. In this case the attached monitor will display the single stream from the appliance in full screen mode.

▼ To connect an Amino directly to an MPEG-2 appliance:

1. Open the management interface on the Amino (**Alt-m**).
2. Navigate to **Browser Setup > Home Page**.
3. In the **Home Page** field, enter the IP address of the VBrick appliance in the following format: **igmp://<vbrick_ipaddress>:port**
4. Reboot the Amino to display the MPEG-2 stream from the VBrick in full screen mode on the monitor.

Configuring the Remote Control for a TV

The Amino handheld IR remote control is designed to work with the Amino set top box. During normal operation, the **STB/TV** button (see the *Portal Server User Guide*) should be set for **STB**. It can, however, be configured to work with a standard TV. In order for the remote to transmit the correct signals to control the TV, it must be programmed with a 3-digit code that matches the TV. See the Amino Remote Controls User Guide for more information.

Configuring the Amino for a Widescreen

This procedure explains how to configure an Amino Set Top Box for MPEG-2 output to a widescreen (16:9) TV. Use one of the following methods depending on whether you are using the handheld remote control or the wireless keyboard. *When done, repeat these steps if necessary for each Amino set top box.*

▼ **To configure for widescreen with the wireless keyboard:**

1. Press **Ctrl** to get into Amino keyboard mode.
2. Press **Alt-p** to get to **Preferences**.
3. On the **Preferences** menu select **TV system and Audio Settings**.
4. Change the **TV Display Format** to **Widescreen TV**.
5. Save changes, exit **Preferences**, and power cycle the STB.
6. Be sure to set the widescreen TV monitor to **Full** mode.

▼ **To configure for widescreen using the remote control:**

1. Select the **Menu** button on the Remote Control to get to **Preferences**.
2. On the **Preferences** menu select **TV system and Audio Settings**.
3. Change the **TV Display Format** to **Widescreen TV**.
4. Save changes, exit **Preferences**, and power cycle the STB.
5. Be sure to set the widescreen TV monitor to **Full** mode.

Setting the TV Display Format

As noted, you can change the **TV Display Format** from the **Preferences** menu. The following tables show the output from normal and widescreen TVs depending on how the **TV Display Format** is set. Be sure to power cycle the STB to implement any changes you make.

Table 16. Video Output with a Normal (4:3) TV:

TV Display Format	Video Output
Standard (4:3) Mode	Normal (4:3) video plays normally and 16:9 video has the left and right sides cropped off (center cutout).
Letterbox Mode	Normal (4:3) video plays normally and 16:9 video has all the picture viewable with black bars on the top and bottom (letterbox).
Widescreen TV	Normal (4:3) video plays normally and 16:9 video displays all the picture but it is squashed in.

© 2007 VBrick Systems, Inc.

Table 17. Video Output with a Widescreen (16:9) TV:

TV Display Format	Video Output
Widescreen TV	16:9 video plays normally and 4:3 video has black bars left and right (pillar box). This relies on the TV responding to aspect ratio switching signals on VBI line 23 (PAL only). On TVs that don't respond to this signal, you must set the TV aspect ratio manually to avoid a stretched or squashed picture.

© 2007 VBrick Systems, Inc.

Chapter 11

ACNS Configuration

Topics in this chapter

Overview 133
ACNS Configuration 133
Verify Installation. 135

Overview

The Cisco Application and Content Networking System (ACNS) is a digital media delivery solution that reduces redundant digital media streaming traffic traversing a WAN from the data center to branch offices over satellite and terrestrial networks. Cisco ACNS offers a comprehensive set of streaming-media features that let you stream high-quality and long-playing digital videos live and simultaneously to thousands of users and media players and provide access on demand at a later time. By caching on-demand content, or prepositioning frequently accessed content, ACNS minimizes the need for the same digital media content to traverse WAN links from the data center to branch offices.

VBrick has partnered with Cisco to integrate VBrick's product line with Cisco's ACNS content distribution system. Integrated VBrick products include encoders, Video on Demand (VOD) servers, Set Top Boxes, PC and MAC clients, and the EtherneTV system. The integration of these two industry-leading products means that customers with legacy networks can retain their existing network infrastructure and still deploy the latest in video delivery systems. The benefits of this product integration include unlimited geographic reach for video, reduced network circuit costs, higher quality video, and improved system performance. Cisco ACNS also provides a flexible management system for efficient operation, automation, and central management of the digital media delivery network.

Note The integrated Portal Server and ACNS Server solution handles MPEG-4 and Windows Media video files residing on Darwin, Windows Media, and VOD-W servers only. MPEG-1 and MPEG-2 files are not supported; VBrick's NXG (Linux) servers are not supported.

ACNS Configuration

To configure the Portal Server to work with ACNS you need to perform certain steps on the Portal Server and on the ACNS server. **If you have a VBrick VOD-W server, you will need to create a virtual directory in IIS before you configure the Portal Server or the ACNS server.** If you have a Darwin server or a Windows Media server, no additional configuration is required.

VOD-W Server Configuration

ACNS copies all MPEG-4 and WM video files from all (Windows Media, Darwin, and VOD-W) servers in your EtherneTV system. (ACNS does not support NXG servers; the

Windows Media and Darwin servers require no additional configuration.) Use the following steps to configure a VOD-W server to work with ACNS.

▼ To configure a VOD-W server to work with ACNS:

1. Login the VOD-W server.
2. Go to **Start > Windows Explorer**.
3. Expand the tree in the left pane under the drive labeled (C:).
4. Expand Program Files under C: and then expand InfoValue under that.
5. Click on **QuickVideo OnDemand Server**.
6. Double-click on the file QvcsSetup.ini. The system should use Notepad to open the file.
7. Locate the line that reads "[Ingest]".
8. Locate the lines beginning with StoragePathN= shortly after the "[Ingest]" line where N is a number. Leave the Notepad window open.
9. Go to **Start > Administrative Tools > Internet Information Services (IIS) Manager.**
10. Expand the tree in the left pane and expand **FTP Sites**.
11. For each StoragePath line found in step 8, configure a virtual directory for it as follows:
    a. Right-click on the **Default FTP Site** and then select **New > Virtual Directory**.
    b. Click **Next** in the Welcome to the Wizard window.
    c. For **Virtual Directory Alias**, enter the text after the first backslash (\) from the StoragePath line whose data is being setup. For example, if the line reads StoragePath1=D:\Content, enter **Content** for the Alias. Click **Next**.
    d. For **FTP Site Content Directory**, click **Browse** and navigate to the directory specified in the StoragePath line whose data is being setup. Click **OK** then **Next**.
    e. In the **Access Permissions** window, click **Next** to select the default permission of Read.
    f. Click **Finish** to complete creation of the new Virtual Directory.

Portal Server Configuration

Portal Server integration with Cisco's ACNS Server is available with Portal Server v4.0.1 or later software. The following procedures explain (1) how to configure a manifest file on the Portal Server that will be used by the ACNS server to ensure that the content on the ACNS Server matches the content on the Portal Server; and (2) how to verify that forced use of TCP for MPEG-4 content is disabled.

▼ To create a manifest file on the Portal Server:

1. Install MCS v4.0.1 or later from the EtherneTV Product CD See the *ETV Portal Server Release Notes* for detailed instructions.
2. After installing the Portal Server, open the Portal Server Admin Console and go to **Global Settings > Global Assignments > Set Cisco ACNS Manifest Options**.
3. Check **Enable manifest generation**, select the files (MPEG-4 and/or WM) to include, and specify an interval (default = 10 minutes) that defines how often the file will be regenerated.
4. Click **Submit** when done.
5. Click **Generate Now** to create an "on demand" manifest file. The Portal Server will create (and periodically overwrite) a manifest file called ACNSManifest.xml in the Program Files\VBrick\MCS\Cisco folder. The Cisco subdirectory is automatically created.

© 2007 VBrick Systems, Inc.

When a Portal Server is configured to integrate with an ACNS network, content playback is redirected to stream from ACNS nodes only if RTSP is used for video transmission. To use RTSP, verify that the Portal Server option to always use TCP is unchecked (this is the default).

▼ To verify that TCP is off:

1. Go to **Global Settings > Global Assignments > Assign LAN/Internet Address Range(s)**.
2. Verify that **Always use TCP protocol (HTTP Tunneling/RTSP Interleaving) for MPEG-4 and Windows Media content?** is unchecked.

ACNS Server Configuration

Note that installation, configuration, and support for ACNS must be provided by Cisco and/or their representatives. Use the following steps to point to the Portal Server manifest file and set other configuration options.

▼ To set configuration options and identify the manifest file:

1. Be sure the ACNS Server is running and launch an Internet Explorer browser.
2. Go to the ACNS Management URL, for example https://<ipaddress>:8443.
3. Log into the ACNS Management Tool.

   Username: admin

   Password: default
4. Click on the **Services** tab at top of page.
5. Create a **Content Channel** for the VOD server.
6. Click on **Channel Content** on the left.
7. Near the top of the screen, set the **content acquisition method** to **specify external manifest file**.
8. In the **Manifest URL** field enter the Portal Server URL in the following format:

   http://<MCSipaddress>/Cisco/ACNSManifest.xml
9. Set the **Check manifest every** field to desired interval (60 minutes is recommended).
10. To check the manifest file, click **Validate** to open a pop-up that will show the manifest. The last message should indicate the manifest is correct.
11. Click **Fetch manifest now** to start content replication.
12. To check the status of the content replication click on **Replication Status** on the left side of page. The system is ready when the following is true:

    Acquisition status is Completed.

    Device states at the screen bottom are Completed, and the In Process counts are zero.

Verify Installation

▼ Use the following steps to verify the MCS/ACNS integration is successful:

1. Be sure that the MCS Portal Server and ACNS are configured as explained above.
2. Go into the ACNS management system and verify that the video content added via the ETV Portal Server has been pushed to the ACNS remote content engine's disk storage.
3. Open a browser and launch a Portal Server client.
4. Launch a stored MPEG-4 or WM video from the Portal Server user interface. The MPEG-4 or WM content should run and play successfully to conclusion.

5. If you run a packet sniffer on the MCS client, a trace will show that the client was redirected to play the content from a Cisco node and not from a VBrick VOD server.

© 2007 VBrick Systems, Inc.

Chapter 12

Rebranding the User Interface

Topics in this document

Customizing the Portal Server 137
Rebranding the Portal Server 138
Rebranding Other ETV Components 142

As explained below, there are two ways to modify the EtherneTV Portal Server user interface. The first method (see Customizing the Portal Server) is to simply replace the title and the header image. This is fairly easy and can be done quickly by a novice administrator. The second way (see Rebranding the Portal Server) is to modify the .css stylesheets and thoroughly rebrand the look-and-feel of the application. This is more complex and requires an administrator or developer who is comfortable working with HTML and .css stylesheets. Note that you can only change the Portal server "user" interface; you cannot change the Admin Console pages.

Customizing the Portal Server

Changing the Title and Header Image

You can change various images on the Portal Server user interface, the VBrick Set Top Box, the Amino set top box, and the WM IP Receiver. On the Portal Server you can also change the default title (VBrick Systems) that is superimposed on the header image (Figure 17). To change this title, open the Portal Server Admin Console and go to **Global Assignments > Change Title**; then enter a new title or leave the title blank by entering at least one space. (Note that the title is always displayed in white text and may not be visible if you use a light-colored background image.) This title change will be retained through subsequent software upgrades. You can also change the header images on the Portal Server and the set top boxes but these changes are not retained when you upgrade the application. *In general, use care when making any changes*. It is always a good idea to copy and save the original image files. For best results, open and view each image in an editor before making any changes.

Figure 17. Header Image

Table 18 shows the images you can change on the Portal Server and the set top boxes. Do not modify or change any other images. You can replace any .jpg image but it must have the same dimensions in pixels (for example 1003x50) as the original image. *It must also have the same security settings*. To view the dimensions and security settings, right-click on the image and select **Properties > Summary** or **Security**. If you are prompted for a user name and password when opening the Portal Server user interface after replacing an image, it is likely that the security profile of the new image does not match the profile of the image you just replaced.

Table 18. EtherneTV Replaceable Images

Interface	Image
Portal Server	Header image: C:\Program Files\VBrick\MCS\Images**topBanner-1003x50_PS.jpg**
VBrick STB	Header image for MCS Portal Server: C:\sfwapp\Components\WebApp\MCS\images\STB**EtherneTV-Top-STB_PS.jpg**
	Header image for MCS Live Portal Server: C:\sfwapp\Components\WebApp\MCS\images\STB**EtherneTV-Top-STB_LPS.jpg**
Amino STB	Header image: C:\sfwapp\Components\WebApp\MCS\MCS_Amino\images**EtherneTV_logo_STB_20.jpg**
	Logo image: C:\sfwapp\Components\WebApp\MCS\MCS_Amino\images**vbrick_logo_stb.gif**
WM IPR	Logo image: C:\sfwapp\Components\WebApp\MCS\WMIPR\banner.jpg

Rebranding the Portal Server

This section explains how to thoroughly change or "rebrand" the look-and-feel of the Portal Server user interface (and the Set Top Box and IP Receiver) by modifying the stylesheets. It addresses the Portal Server "user" interface only—not the Admin Console. The Portal Server stylesheets are located at C:\Program Files\VBrick\MCS\css. It is always a good practice to backup all files that you will be changing and to thoroughly test your results before you are finished. *This section describes some user interface elements that are only available in Portal Server v4.2 or higher.* If you have an earlier version, you can modify the corresponding classes present in your version.

Note The stylesheet changes listed below are not saved when you upgrade the Portal Server application. You can save and reapply your changed stylesheets but be aware that a subsequent upgrade may have additional .css classes.

Portal Server

Webpage Background

Files to Change	css/MCSv4.css
Classes	body{}
Modify	Any background attribute to fit your requirements.
Example	Changing background image to color only (remove the background-image: tag and adjust the background-color: tag to your color in Hexadecimal (#ffffff) or by Color Name (White).

Header Image

Files to Change	css/PC_HighRes.css, css/PC_LowRes.css
Classes	#header, .headerLogo

© 2007 VBrick Systems, Inc.

Modify	#header tag – add: background-image: url(yourLogo.jpg); .headerLogo – change to: display:none;

Header Client Branding

(Left hand text in header)

Files to Change	css/MCSv4.css
Classes	.header_ClientBranding
Modify	Any attributes for font and color.

Page Margins and Borders

Files to Change	css/PC_HighRes.css, css/PC_LowRes.css
Classes	#workspace
Modify	Any attributes for margins, positioning, borders and master workspace background color/image.

Header Search Bar Background

Files to Change	css/PC_HighRes.css, css/PC_LowRes.css
Classes	#searchbar
Modify	Any attributes.

Header Search Bar Navigation Text

Files to Change	css/MCSv4.css
Classes	.searchbar_main_button
Modify	Font, color.

Header Search Bar

Files to Change	css/MCSv4.css
Classes	.formtext_bold, .imagebutton, .searchbox
Modify	Font, color, etc.

Header Search Bar Time

Files to Change	css/MCSv4.css
Classes	.clock
Modify	Font, color, etc.

Player's Title Text

Files to Change	css/MCSv4.css
Classes	.player_titlebar_text
Modify	Font, color, etc.

Channel Guide Search TextBox

Files to Change	css/ChanGuide_styles.css
Classes	.CHGuideSearchTextBox
Modify	Font, color, etc.

Channel Guide Background Search Area

Files to Change	css/ChanGuide_styles.css
Classes	.timeHeadertableSearch
Modify	Background-color

Channel Guide Time Navigation

Files to Change	css/ChanGuide_styles.css
Classes	.timeHeadertable, .timeHeaderCells, .CHGuidePrevBtn, .CHGuideNextBtn
Modify	Background-color, color, fonts, etc.
Button Images	/ChannelGuideImages/leftArrow.gif, /ChannelGuideImages/ rightArrow.gif

Channel Guide Program Menu Text

Files to Change	css/ChanGuide_styles.css
Classes	.ChGuideProgramMenuTitle, .ChGuideProgramMenuDesc, .ChGuideProgramMenuItemTitles, .ChGuideProgramMenuItemDesc, .ChGuideProgramMenuDescRecord, .ChGuideProgramMenuDescSchedule
Modify	Color, font, padding, etc.

Channel Guide Program Menu Background

Files to Change	css/ChanGuide_styles.css
Classes	.CHMenu
Modify	Background-color, background-Image, etc.

© 2007 VBrick Systems, Inc.

Channel Guide Station Menu

Files to Change	css/ChanGuide_styles.css
Classes	.ChGuideStationMenuPosition, .ChGuideStationMenuTable, .ChGuideStationMenuChannel, .ChGuideStationMenuTitle
Modify	Background-color, background-Image, fonts, color, dimensions, etc.

Channel Guide Content List

Files to Change	css/ChanGuide_styles.css
Classes	.ChguideTable, .ChGuideStationCells, .ChguideCells, .ChguideCellsRecording
Modify	Border, color, background-color, recording image, padding, etc.

Live Content List

Files to Change	css/PC_HighRes.css, css/PC_LowRes.css
Classes	.ContentList
Modify	Border, background-color, scroll-bar.

Footer

Files to Change	css/PC_HighRes.css, css/PC_LowRes.css, MCSv4.css
Classes	#menu, .menuitem
Modify	Color, background-color, fonts, size, etc.

Messages Area

Files to Change	css/PC_HighRes.css, css/PC_LowRes.css
Classes	#messages, message_box_text
Modify	Positioning, background-image, color, font dimensions.

Items in Current Playlist

Files to Change	css/PC_HighRes.css, css/PC_LowRes.css, css/MCSv4.css, css/MCSControls.css
Classes	.PlaylistAdminContentList, .PlaylistAdminDiv, .btn_varWidth, v4DataProgramTitle, .SubtitleCell, .MenuCell, .MenuItem
Modify	Font, color, background-color, dimensions.

Rebranding Other ETV Components

VBrick Set Top Box

STB List and Related HTML

Files to Change	css/MCS_Styles_stb.css, layers/mainElement-background-stb.inc
Classes	all
Modify	Font size, color, background, padding, etc.
HTML	Any files in: layer/ directory ending with "–stb.inc"

Amino Set Top Box

STB List and Related HTML

Files to Change	MCS_Amino/css/A_classes.css, A_layout.css, MCSControls.css
Classes	All
Modify	Font size, color, background-color, dimensions, padding, etc.

VBrick IP Receiver

IPR List and Related HTML

Files to Change	WMIPR/css//wmipr.css
Classes	All
Modify	Font size, color, background, padding, etc.

© 2007 VBrick Systems, Inc.

Chapter 13

NXG-to-VOD-W Content Migration

Topics in this document

Creating an Asset List 143
Using the Migration Tool. 144
Verifying the Migration 147

This chapter explains how to migrate MPEG-1 and MPEG-2 video files from a VBrick NXG (Linux) VOD server to a VBrick VOD-W (Windows) VOD server. This migration is a two-step process:

▼ To migrate NXG files:

1. First run the Linux script VBListAssets.sh on the NXG VOD server to create an asset list that identifies all video files present on the server.
2. Then run the migration tool to replicate these files on the VOD-W server.

Creating an Asset List

Use the steps listed below to run a script that will create an asset list (see Sample Asset List) of all video files on the NXG server. **The script requires that the following files be FTPed to the NXG server.** These files are located in the Portal Server utilities folder at: C:\Program Files\Vbrick\MCS\utils\NXGtoVODWMigrationTools

VBListAssets.awk

VBListAssets.sh

▼ To run the script, FTP the files listed above to the NXG server:

1. Open a Command Prompt on your PC and change directories to the folder with the files listed above.

   FTP <NXG_ip_address>
2. Login as user = **vbrickuser**; password = **vbrickuser**

   ftp> **bin** to transfer the files in binary mode.

   ftp> **mput VBL*** to transfer the script to the server. When prompted, answer **y** to allow the file transfer.

   ftp> **quit** to exit FTP.
3. Telnet to the NXG server to run the script.

   telnet <NXG_ip_address>
4. Login as user = **vbrickuser**; password = **vbrickuser**

   chmod 777 VBL* to make the script files executable (FTP will not do this).

   ./VBListAssets.sh to run the script.
5. Wait approximately two minutes until the script completes. When prompted for password, type the root password (default = **omnibase**) and press **Enter**. The file

nxg_asset_list will be created in the current directory. The script should not generate any output. If it does, note the output for analysis by VBrick Support Services.

6. Copy nxg_asset_list to the Portal Server machine or use an FTP URL in the **Assets** field of the Migration Tool. For example:
   ftp://vbrickuser:vbrickuser@<server_ip_address>/nxg_asset_list

Sample Asset List

This snippet shows sample assets included in the file nxg_asset_list. Each asset is described by name and location.

```
<assets>
  <asset>
    <name>/demo/TestAutoIngest4.mpg</name>
    <location>/vbrick/content_links/20071005113535_1</location>
  </asset>
  <asset>
    <name>/1_MSNBC_05_16_07_16_12_41.mpg</name>
    <location>/vbrick/content_links/20071005113535_2</location>
  </asset>
  <asset>
    <name>/Rec9.mpg</name>
    <location>/vbrick/content_links/20071005113535_3</location>
   </asset>
 </assets>
```

Using the Migration Tool

The Migration Tool is used to migrate MPEG-1 and MPEG-2 video files from a VBrick NXG VOD server to a VBrick VOD-W VOD server. The original content remains on the NXG server and is not affected. The Migration Tool is a Windows-based application that is installed with the Portal Server installation and should be run on the Portal Server machine. Once you have created an asset file, use the following steps to actually migrate files to the VOD-W server. Note that the ingestion process on the VOD-W server is CPU and bandwidth intensive. You may want to run the migration during off-peak hours and increase the ingestion rate as explained below. Be sure to read the following important notes.

Note

- Both the **Source** and **Destination** VOD servers must be defined in MCS and must be running.
- You must create an MCS user (or configure MCSClient, the default user) that can access the **Destination** VOD-W server but *cannot* access the **Source** NXG server. See Configuring Users on page 91 for details. The MCS user must be configured as follows.
  - Allow Access to Specific VOD Servers – select only the destination VOD-W.
  - Allow Access to Specific VOD Content – select all VOD Folders.
  - Allow Content Publishing – select all Available Folders.
- The Migration Tool will not run if SSL is enabled on the Portal Server. To disable SSL, re-comment the web.config file for Portal Server User pages *and* the Portal Server Admin pages. See Configuring for SSL on page 103 for details.

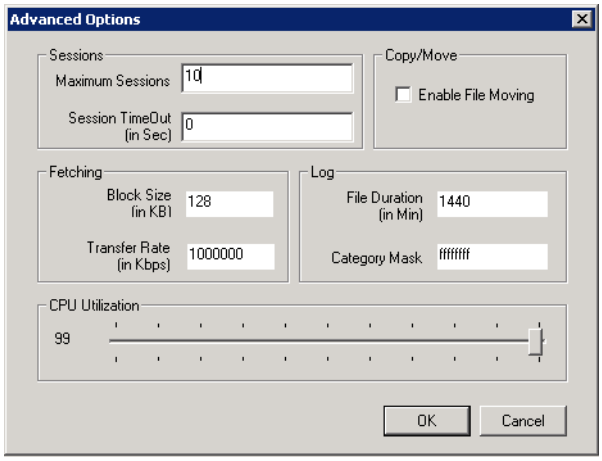
© 2007 VBrick Systems, Inc.

Increasing the Ingestion Rate

You can make the migration process substantially faster by increasing the rate at which files are ingested on the VOD-W server.

▼ To increase the ingestion rate:

1. On the VOD-W server, go to **Start > Control Panel > InfoValue QuickVideo > QVCS > Advanced**.

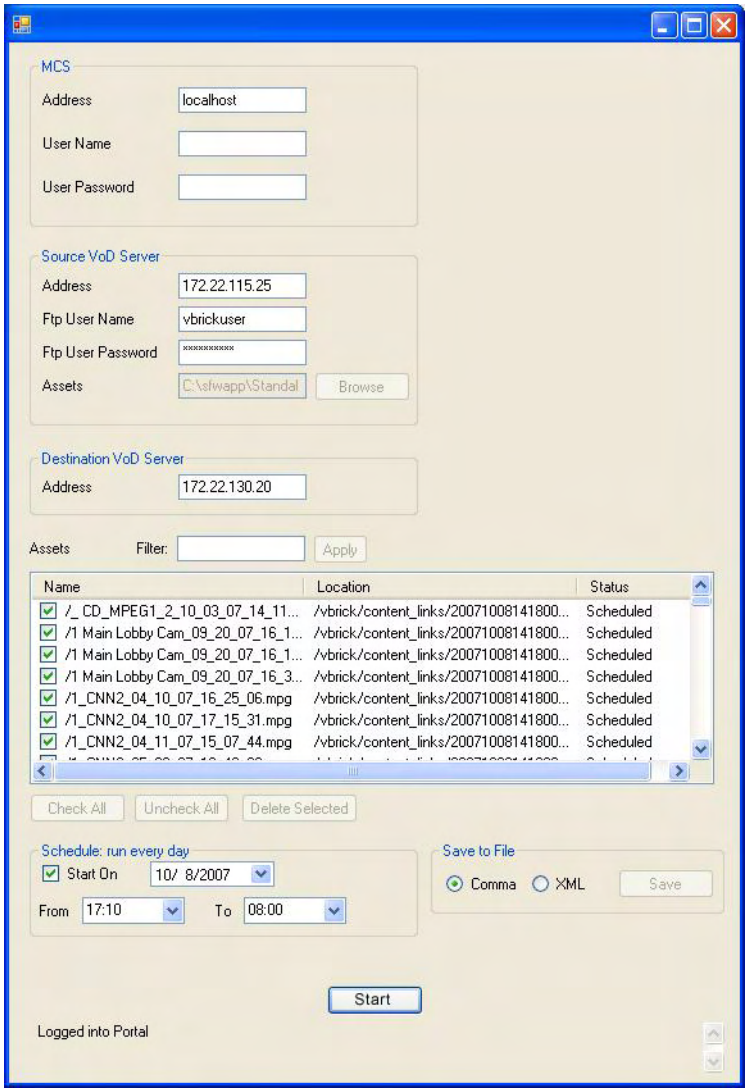


2. Set the **Transfer Rate** to **1000000** and click **OK**. Click **OK** again to exit.
3. When the content migration is complete, reset the **Transfer Rate** to the default (**10000**).

Running the Migration Tool

▼ To migrate video files to the VOD-W:

1. Launch the Migration Tool. Go to C:\Program Files\Vbrick\MCS\utils\NXGtoVODWMigrationTools and double-click on VBMCSReplicateContent.exe
2. Complete all required fields as explained below.
3. Select **Save to File** to create a status file that will show which files were ingested successfully.
4. Click **Start** to begin the migration immediately, or use the scheduling options to run later.
5. If necessary, when the content migration is complete, reset the **Transfer Rate** to the default (**10000**).



MCS	
Address	IP address of VBrick Portal Server.
User Name	User name for Portal Server.
User Password	User password for Portal Server.
Source VoD Server	
Address	IP address of source NXG server.
Ftp User Name	FTP user name of NXG server. Default = vbrickuser
Ftp User Password	FTP password of NXG server. Default = vbrickuser
Assets	Browse to the file nxg_asset_list or use an FTP URL in the following format: ftp://vbrickuser:vbrickuser@<server_ip_address>/nxg_asset_list
Destination VoD Server	
Address	IP address of destination VOD-W server.

© 2007 VBrick Systems, Inc.

Assets	
Filter	Optional. Enter an alphabetic substring to search for matching files and click **Apply**.
File Names	Select the video files to be migrated from the complete list of files in the asset list. Use **Check All**, **Uncheck All**, or **Delete Selected** as appropriate. Note that **Delete Selected** works with selected (i.e. highlighted) files and *not* checked files.
Schedule	
Start On	Start date. Default = unchecked. The tool will migrate files every day beginning at the specified hour.
From/To	The migration will run during the specified time period.
Save to File	This option saves a status.xml file that shows migration results. If some files fail to ingest during migration, you can point to this file in the **Assets** field and repeat the migration. • Comma – save the status file as comma separated values. This can be displayed in a spreadsheet or an editor. • XML – save status file as an .xml file. This file is identical in format to the asset list (see Sample Asset List) and can be used to repeat the migration.
Start/Stop	Start a migration; stop a migration currently in progress. You may want to stop the migration and correct a problem if multiple failures are shown in the Status column. See Recovering from Migration Errors below.

Recovering from Migration Errors

Migration errors are shown in the **Status** column. Once started, the migration will continue until each ingestion reports either success or failure. If you stop the migration, all queued ingestions are removed (click yes on the popup) from the Portal Server and you can correct the errors and restart the migration when ready.

If you ignore the popup window (click no on the popup), you will have to either remove queued ingestions manually from the Portal Server or wait until all ingestions are complete with either failure or success. Then you can fix the errors and restart. You may see duplicate asset file errors in the migration **Status** column. These errors indicate that the asset already exists on VOD-W and the Portal Server and can be safely ignored.

Verifying the Migration

Use the **Save to File** (XML) option to create a status.xml file which lists the video files that failed to ingest. If some files fail to ingest during migration, you can point to this file in the **Assets** field and repeat the migration.

© 2007 VBrick Systems, Inc.

Index

Numerics

1. Generate a Certificate Request 103
1. Setup and Configure the EtherneTV System 89
2. Choose an Authentication Method 89
2. Submit a Certificate Request 104
3. Install the Certificate 104
4. Configure ETV Resources for SSL 105
4. Create Resource Groups on the Portal Server 91
5. Create Users on the ETV Portal Server 91

A

Access Control 76
Access Logging 61
Add Link 70
Add/Modify a URL for a Live Video Stream 52
Add/Modify Group's Resource Assignments 98, 100
Add/Modify Group's User Assignments 98
Add/Modify Resource Group Information 99
Add/Modify User's Resource Assignments 100
Admin Console Login 15
Advanced Settings 38
Allow Access to Specific FTP Servers 95
Allow Access to Specific Recorder Servers 95
Allow Access to Specific VOD Content 95
Allow Content Publishing 96
Allow Content Recording 96
Allow VBrick Access 96
Authentication by IP Address 101
Authentication by PIN 100
Authentication 88
Authorization 88
AutoIngest Content 119
AutoIngest Content via XML 121

C

Configuring a Presentation User 114
Configuring for Live Presentations 115
Configuring for Presentations 114
Configuring for Stored Presentations 117
Configuring IWS for Control Devices 43
Configuring the Amino 128
Connecting Control Devices 42
Connecting the Amino 127
Control Devices 38
Copyright Restrictions & Expiration Privileges 97
Copyright Restrictions and Content Expiration 3
Creating a Script 50
Custom Fields 25

D

Database Backup 125
Default Content Recording 96
Defining Custom Control Devices 41
Definitions 87
Desktop Requirements 2
Diagnostics 75
Download Components 10

E

Emergency Broadcast 55
Emergency Broadcast Privileges 97
End User Features 4
EtherneTV Video-on-Demand Servers 6
EtherneTV-STB Set Top Box 8
ETV Internet-Based Servers 7
ETV Network Video Recorder 8
Example 51
Expired Content Log 76
Extended Logging Properties 62

G

Global Assignments 19

H

Help 84

I

Installing the Root Certificate 81
Introduction 125

L

Launching a Live Presentation 115
Launching a Stored Presentation 117
LDAP 88
License Files 14
Live Presentations 83
Locked-Down Windows PCs 11
Logout 85

M

Macintosh and Linux PCs 11
Managing Rich Media Presentations 113

Modify VOD Content 73
MySQL 4

O

Overview 1, 87

P

Port Requirements 12
Portal Server Components 6
Portal Server Installation 10
Program Names 59

R

Recorders 46
Removing a Live Presentation 116
Resolving Other Security Alerts 83
Resource Groups 84
Resources and Resource Groups 88

S

Schedule Privileges 97
Script Devices 48
Scripts 49
Securing the Portal Server User Pages 105
Server Requirements 2
Servers 27
Set Top Boxes 44
Status 75
STB Access 96
STB Authentication 100
Stream Restrictions 26
Synchronizing the Portal Server and the NVR 47

U

User Groups 84
Users 84
Users 91
Using LDAP Servers with SSL 81
Using Single Sign-On 79
Using the XML Template 122

V

VB-PC Remote Controller 9
VBrick Database 88
VBrick Encoders/Decoders 6
VBricks 36

W

Windows PCs 10
Working with Presentations 114

Z

3. Create User Groups on the Portal Server 90
6. Assign Resources to Users or User Groups 91
Add Non-VOD Content 55
Add VOD Content 54
Add/Modify Group Information 98
Add/Modify Live Channel Privileges 94
Add/Modify User Information 93
Add/Modify User's Group Assignments 94
Add/Modify User's Resource Group Assignments 94
Add/Modify Video On Demand Content Folders 34
Add/Modify VOD/FTP Servers 28
Admin Console Options 16
Administrative Features 5
Allow Access to Specific VOD Servers 95
Allow Viewing by Content Type 95
Database Restore 126
LDAP Directory Server 90
Overview 103
Removing MPEG-4 Closed Captions 124
Resource Groups 99
Securing the Portal Server Admin Pages 105
URLs 52
User Groups 97
VBrick Database 90
Assigning Privileges to Users 94

VBrick Systems, Inc.
12 Beaumont Road
Wallingford, Connecticut 06492, USA